CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Universiti Putra Malaysia Institutional Repository

Malaysian Journal of Mathematical Sciences 9(S) June: 71-88 (2015)
Special Issue: The 4th International Cryptology and Information Security Conference 2014 (Cryptology 2014)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES
Journal homepage: http://einspem.upm.edu.my/journal

Pseudo τ - Adic Non Adjacent Form for Scalar Multiplication on Koblitz Curves

Faridah Yunos, *Kamel Ariffin Mohd Atan, Muhammad Rezal Kamel Ariffin and Mohamad Rushdan Md Said

Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

E-mail: faridahy@.upm.edu.my

*Corresponding author

ABSTRACT

In ECC, scalar multiplication is the dominant operation, namely computing nP from a point P on an elliptic curve where the multiplier n is an integer, defined as the point resulting from adding $P + P + \cdots + P$, n times. The τ-NAF proposed by Solinas, is one of the most efficient algorithms to compute scalar multiplications on Koblitz curves. In this paper, we introduced an equivalent multiplier to τ-NAF namely pseudoTNAF. It is based on the idea of transforming the τ-NAF expression to a reduced τ-NAF that has been done by some researchers. It can eliminate the elliptic doublings in scalar multiplication method, and double the number of elliptic additions. We provide the formula for obtaining a total of lattice points in Voronoi region of modulo $r + s\tau$ where $r + s\tau$ an element of ring $Z(\tau)$. This helps us to find all the multipliers n that based on τ-NAF. We also discuss the estimation of operational costs when using pseudoTNAF as a multiplier of scalar multiplication

Keywords: Scalar multiplication, Koblitz curve, density, Voronoi region, Hamming weight.

1. INTRODUCTION

The Koblitz curves are a special type of curves for which the Frobenius endomorphism can be used for improving the performance of

computing a scalar multiplication (Koblitz,1987). The Koblitz curves are defined over F_2 as follows

$$E_a: y^2 + xy = x^3 + ax^2 + 1$$

where $a \in \{0,1\}$ (Koblitz, 1992). The Frobenius map $\tau: E_a(F_{2^m}) \mapsto E_a(F_{2^m})$ for a point $P = (x, y)$ on $E_a(F_{2^m})$ is defined by

$$\tau(x, y) = (x^2, y^2) \ , \qquad \tau(O) = O$$

where O is the point at infinity. It stands that $(\tau^2 + 2)P = t\tau(P)$ for all $P \in E_a(F_{2^m})$, where the trace, $t = (-1)^{1-a}$. Thus, it follows that the Frobenius map can be considered as a multiplication with complex number $\tau = \frac{t+\sqrt{-7}}{2}$ (Solinas, (2000)).

In the ensuing discussion, the following definitions will be applied.

Definition 1. (Yunos and Mohd Atan, 2013**).** A τ-adic Non-Adjacent Form of nonzero $\bar{n}$ an element of $Z(\tau)$ is defined as $\tau\text{-}NAF(\bar{n}) = \sum_{i=0}^{l-1} c_i \tau^i$ where l is the length of an expansion of $\tau\text{-}NAF(\bar{n})$, $c_{l-1} \neq 0$, $c_i \in \{-1,0,1\}$ and $c_i c_{i+1} = 0$.

Definition 2. (Yunos and Mohd Atan, 2013**).** A Hamming weight is defined as the number of elements -1 and 1 of an expansion of an element of $Z(\tau)$**.**

Definition 3. (Hankerson et al., 2004). Let $N: Z(\tau) \rightarrow Z$ as a function of norm and $\alpha = x + y\tau$ an element of $Z(\tau)$. The norm of α is $N(\alpha) = x^2 + txy + 2y^2$ where $t = (-1)^{1-a}$.

Definition 4. An operational costs is defined as the cost in terms of running time to compute the scalar multiplication of the number of doubling and addition operations.

Definition 5. (Solinas, 2000). Let $\lambda \in Q(\tau)$, and $\lambda = \lambda_0 + \lambda_1\tau$ with λ_0, $\lambda_1 \in R$. U is a region in the (λ_0, λ_1)-plane by the inequalities below.

$$-1 \leq 2\lambda_0 + t\lambda_1 < 1$$
$$-2 \leq \lambda_0 + 4t\lambda_1 < 2$$
$$-2 \leq \lambda_0 - 3t\lambda_1 < 2.$$

Definition 6. A Voronoi region of $\psi\, Z(\tau)$ is denoted by

$$\mathrm{V} = \{\lambda\, \psi : \lambda \in\ U, \psi \in\ Z(\tau)\}.$$

In this paper, we introduced an equivalent multiplier to τ-NAF namely pseudoTNAF. This is based on the idea of transforming the τ-NAF to a reduced τ-NAF developed by some researchers for example Solinas, 2000, and Joye and Tymen, 2001. We begin in Section 2 with the concept of reduction in the ring Z(τ). In Section 3, we prove the equivalence of both expansion of τ-NAF and pseudoTNAF, also refined one of the properties of ρ so that the scalar multiplication is not heading to infinity. Two other properties have been discussed by Yunos et al., 2014. In Section 4, we give the formula to find the number of elements in Voronoi region of $\rho\frac{\tau^m - 1}{\tau - 1} Z(\tau)$ and produced the algorithm for finding all points in mod $(r + s\tau)$. This algorithm is important to facilitate the process of getting all pseudoTNAF for all elements in $\rho\ \frac{\tau^m - 1}{\tau - 1}$ developed in Section 5. The discussion concluded with the estimating of average Hamming weight of pseudoTNAF with maximum length.

2. MODULO REDUCTION IN Z(τ)

The region U that was mentioned in Definition 5 form a hexagon with six vertices with their norms $\frac{4}{7}$ respectively. If the vertices is represented by $\lambda = \lambda_0 + \lambda_1\tau$ then $\lambda_0^2 + t\,\lambda_0\lambda_1\,\tau + 2\,\lambda_1^2 = \frac{4}{7}$ form an ellipse. However, if λ a point in the ellipse, then the norm is less than $\frac{4}{7}$. Thus, we have

$$N(\lambda) \leq\ \tfrac{4}{7}.$$

The rounding process of $\lambda \in\ Q(\tau)$ is done via

$$Round(\lambda) = \left\lfloor \lambda + \frac{1}{2} \right\rfloor \tag{1}$$

so that $\lambda \in Z\ (\tau)$. The value of $\left\lfloor \lambda + \frac{1}{2} \right\rfloor$ is the largest integer that does not exceed $\lambda + \frac{1}{2}$.

The reduction concept in the field of rational integer has been discussed by Solinas, 2000. The reduction of $x' mod\, z'$ is expressed as $x' \equiv y' mod\, z'$ where y' and $z' > 1$ are integers, $-\frac{z'}{2} \leq x' < \frac{z'}{2}$ and $N(x') < \frac{1}{2}N(z')$. This reduction is then expanded to the ring of $Z(\tau)$ i.e.

$$x'' \equiv y'' mod\ z''$$

where y'' and z'' are elements of $Z(\tau)$. Division y'' by z'' produces the residue x'' and it can be written as

$$y'' = \kappa\, z'' + x''$$

where $\kappa \in Z(\tau)$. Suppose that $\lambda = \frac{y''}{z''}$. It generates λ an element of $Q(\tau)$. The rounding process of λ to an element of $Z(\tau)$ is done via (1) so that κ an element of $Z(\tau)$. Therefore, the residue x'' is obtained from equation

$$x'' = y'' - \kappa\, z''$$

where $\kappa = Round(\lambda)$. Now, the above expression becomes

$$x'' = z''(\lambda - Round(\lambda))$$

where $N\big(\lambda - Round(\lambda)\big) \leq \frac{4}{7}$. To avoid scalar multiplication towards to infinity, the residue x'' must have a norm as small as possible i.e.

$$N(x'') \leq \frac{4}{7}N(z''). \tag{2}$$

ROUTINE 62 in Solinas, 2000, for division in $Z(\tau)$ provides a detail reduction steps for $x'' mod\, z''$. This algorithm has been used by Solinas in the reduction of $x'' mod\, (\tau^m - 1)$ and $x'' mod\, \frac{\tau^m - 1}{\tau - 1}$..

3. EQUIVALENCE OF τ-ADIC NAF

The main purpose of obtaining an equivalence of τ –adic NAF is to maintain the situation so that the doubling operation in elliptic scalar multiplication method can be eliminated and the number of elliptic additions can be doubled. Let G be a set of points on Koblitz Curve. Let γ and β are element of $Z(\tau)$ such that $\gamma P = \beta P$ for all $P \in G$. Therefore τ –NAF(γ) is

equivalent to τ –NAF(β) with respect to G. The following proposition provides a guideline on how the equivalence of two τ –NAF occur on the entire set $G = E_a F_{2^m}$.

Proposition 1. If γ, β and ρ are elements of $Z(\tau)$ where $\gamma \equiv \beta \, mod \, \rho \frac{\tau^m - 1}{\tau - 1}$ then $\gamma P = \beta P$ for all $P \in E_a F_{2^m}$. τ – NAF(γ) is equivalent to τ – NAF(β) in set $E_a F_{2^m}$.

Proof.

Given γ, β and ρ are elements of $Z(\tau)$ and $\gamma \equiv \beta \, mod \, \rho \frac{\tau^m - 1}{\tau - 1}$. Therefore,

$$\gamma = \beta + \rho \frac{\tau^m - 1}{\tau - 1} \cdot \kappa$$

for $\kappa \in Z(\tau)$. Thus,

$$\gamma P = \beta P + \rho \frac{\tau^m - 1}{\tau - 1} \cdot \kappa \cdot P.$$

Since $(\tau^m - 1)P = O$ (refer Proposition 65 on page 221 Solinas, 2000, then

$$\gamma P = \beta P + O$$
$$\gamma P = \beta P.$$

Hence, τ – NAF(γ) is equivalent to τ –NAF(β) in set $E_a F_{2^m}$. ■

In this paper, γ as a product of reduction modulo $\rho \frac{\tau^m - 1}{\tau - 1}$ as shown in Proposition 1 can be used as a multiplier for P. If the multiplier of P is equal to $\rho \frac{\tau^m - 1}{\tau - 1}$, then the scalar multiplication getting towards infinity due to

$$\rho \frac{\tau^m - 1}{\tau - 1}(P) = (\tau^m - 1) P \cdot \frac{\rho}{\tau - 1} = O.$$

To avoid this situation, $\gamma \in Z(\tau)$ with the norm as small as possible should be selected. Solinas, 2000, has given condition (2) of $N(x')$ for $x'' \equiv y'' mod \, z''$ for any $z'' \in Z(\tau)$. With this guideline, the following condition must be chosen. That is,

$$N(\gamma) \leq \frac{4}{7} N\left(\rho \frac{\tau^m - 1}{\tau - 1}\right). \quad (3)$$

This study named the τ –NAF(γ) with condition (3), $\rho \neq 1$ and $\rho \neq \tau - 1$ as pseudo τ –adic non adjacent form of γ and abbreviated as pseudoTNAF(γ).

By substituting γ with $\bar{n}$, pseudoTNAF($\bar{n}$) can be used in place of τ-NAF($\bar{n}$) for elliptic scalar multiplication on the set $E_a\, F_{2^m}$. The elliptic operational costs with pseudoTNAF($\bar{n}$) can be calculated by estimating an average Hamming weight of it's expansion. Such average is a product of multiplying an average density among pseudoTNAF($\bar{n}$) that have the maximum length $\bar{l}$ by the size of maximum length.

4. VORONOI REGION OF $\rho\frac{\tau^m-1}{\tau-1}Z(\tau)$

In this section, we give a geometric description of element n that is a result from the modulo reduction of $\rho\frac{\tau^m-1}{\tau-1}$. The following theorem is important in order to get the Voronoi region of $\rho\frac{\tau^m-1}{\tau-1}Z(\tau)$ where $\rho\frac{\tau^m-1}{\tau-1} \neq 0$.

Theorem 1. Suppose that λ is in the interior of region U, $\psi = r + s\,\tau$ and $\omega = N(\psi)$. Then the following properties are true for every nonzero $\psi \in Z(\tau)$.

(i) If $N(\lambda) < N(\lambda \pm \psi)$ then $|(2r+ts)\lambda_0 + (tr+4s)\lambda_1| < \omega$.
(ii) If $N(\lambda) < N(\lambda \pm \tau\psi)$ then $|(r-3ts)\lambda_0 + (4tr+2s)\lambda_1| < 2\omega$.
(iii) If $N(\lambda) < N(\lambda \pm \bar{\tau}\psi)$ then $|(r+4ts)\lambda_0 - (3tr-2s)\lambda_1| < 2\omega$.

Proof.

Suppose that $\lambda = \lambda_0 + \lambda_1\tau$ and $\psi = r + s\,\tau$.

(i) If $N(\lambda) < N(\lambda + \psi)$ then we have

$$\lambda_0^2 + t\lambda_0\lambda_1 + 2\lambda_1^2 < \lambda_0^2 + 2\lambda_0 r + r^2 + t(\lambda_0\lambda_1 + \lambda_0 s + r\lambda_1 + rs) + 2(\lambda_1^2 + 2\lambda_1 s + s^2)$$
$$0 < \lambda_0(2r+ts) + \lambda_1(tr+4s) + (r^2 + trs + 2s^2)$$
$$-(r^2+trs+2s^2) < \lambda_0(2r+ts) + \lambda_1(tr+4s)$$
$$-N(\psi) < \lambda_0(2r+ts) + \lambda_1(tr+4s).$$

Take $N(\psi) = \omega$, then we have

$$-\omega < \lambda_0(2r+ts) + \lambda_1(tr+4s). \tag{4}$$

And also by using the similar way as above, if $N(\lambda) < N(\lambda - \psi)$, then

$$\omega > \lambda_0(2r + ts) + \lambda_1(tr + 4s). \quad (5)$$

From (4) and (5), we obtain

$$-\omega < \lambda_0(2r + ts) + \lambda_1(tr + 4s) < \omega.$$

(ii) If $N(\lambda) < N(\lambda + \tau\psi)$, then

$$\begin{aligned}\lambda_0^2 + t\lambda_0\lambda_1 + 2\lambda_1^2 < \lambda_0^2 - 4\lambda_0 s + 4s^2 + \\ t(\lambda_0\lambda_1 + \lambda_0 r + \lambda_0 st - 2\lambda_1 s - 2rs - 2s^2 t) \\ +2(\lambda_1^2 + 2\lambda_1 r + 2\lambda_1 st + r^2 + 2rst + s^2) \\ 0 < \lambda_0(tr - 3s) + \lambda_1(4r + 2st) + 2(r^2 + trs + 2s^2) \\ -2\omega < \lambda_0(tr - 3s) + \lambda_1(4r + 2st). \quad (6)\end{aligned}$$

And also by using the similar way as above, if $N(\lambda) < N(\lambda - \tau\psi)$, then we get

$$2\omega > \lambda_0(tr - 3s) + \lambda_1(4r + 2st). \quad (7)$$

From (6) and (7), we obtain

$$-2\omega < \lambda_0(tr - 3s) + \lambda_1(4r + 2st) < 2\omega.$$

Since $\frac{1}{t} = t$ for $t = \pm 1$ then

$$-2\omega < \lambda_0(r - 3ts) + \lambda_1(4tr + 2s) < 2\omega.$$

(iii) If $N(\lambda) < N(\lambda + \bar{\tau}\psi)$, then

$$\begin{aligned}\lambda_0^2 + t\lambda_0\lambda_1 + 2\lambda_1^2 < \lambda_0^2 + 2t\lambda_0 r + 4\lambda_0 s + 4s^2 + 4trs \\ +t(\lambda_0\lambda_1 - \lambda_0 r + t\lambda_1 r - tr^2 + 2\lambda_1 s - 2rs) + \\ 2(\lambda_1^2 - 2\lambda_1 r + r^2) \\ 0 < \lambda_0(tr + 4s) + \lambda_1(-3r + 2ts) + 2(r^2 + trs + 2s^2) \\ -2\omega < \lambda_0(tr + 4s) + \lambda_1(-3r + 2ts) \quad (8)\end{aligned}$$

And also by using the similar way as above,, if $N(\lambda) < N(\lambda - \bar{\tau}\psi)$, then we have

$$2\omega > \lambda_0(tr + 4s) + \lambda_1(-3r + 2t) \quad (9)$$

From (8) and (9), we obtain

$$-2\omega < \lambda_0(tr + 4s) + \lambda_1(-3r + 2ts) < 2\omega.$$

Since $\frac{1}{t} = t$ for $t = \pm 1$ then

$$-2\omega < \lambda_0(r + 4ts) + \lambda_1(-3tr + 2s) < 2\omega. \quad \blacksquare$$

As a result, the Voronoi region of $\psi\, Z(\tau)$ is given by the inequalities

$$\begin{aligned} -\omega \le (2r + ts)\lambda_0 + (tr + 4s)\lambda_1 < \omega \\ -2\omega \le (r + 4ts)\lambda_0 - (3tr - 2s)\lambda_1 < 2\omega \\ -2\omega \le (r - 3ts)\lambda_0 + (4tr + 2s)\lambda_1 < 2\omega. \end{aligned}$$

The above result is similar to the definition of region V made by Solinas, 2000, with the assumption of the variable w is the norm of $\psi = \frac{\tau^m - 1}{\tau - 1}$. Whereas, in our study, w is the norm of any element in $Z(\tau)$. However, this study has confirmed that the definition of V made by him can be apply to the case of ψ is any element in $Z(\tau)$. There is suggestion in Theorem 6 of Gordon, 2008, say that the elements in the Voronoi region with $\tau^m - 1$ can be obtained from the distribution of elements in $L = \{0,1,2,\ldots, N(\tau^m - 1) - 1\}$ by $\tau^m - 1$. In other words, the reduction of L mod $\tau^m - 1$ produces a total of $N(\tau^m - 1) - 1$ distinct lattice points in the Voronoi region of $(\tau^m - 1)\mathrm{Z}(\tau)$. Solinas (2000) also follow the same suggestion i.e. the Voronoi region with $\frac{\tau^m - 1}{\tau - 1}$ can be derived from the division of each element in $\left\{0,1,2,\ldots, N\left(\frac{\tau^m - 1}{\tau - 1}\right) - 1\right\}$ by $\frac{\tau^m - 1}{\tau - 1}$. This division also generates a total of $N\left(\frac{\tau^m - 1}{\tau - 1}\right)$ distinct lattice points. This is reinforced with Proposition 75 of Solinas, 2000, which says that the lattice points in the region Voronoi is exactly $n \bmod \psi$ for any $\psi \in Z(\tau)$ where $0 \le n < N(\psi)$. The question now, does this proposition could be applicable in the case of $\psi = \rho\frac{\tau^m - 1}{\tau - 1}$? Suppose that Voronoi region with $\rho\frac{\tau^m - 1}{\tau - 1}$ and written as $V = \left\{\rho\frac{\tau^m - 1}{\tau - 1}\lambda : \lambda \in U\right\}$. The following describes the Voronoi region of $2\frac{\tau^3 - 1}{\tau - 1}Z(\tau) = (-2 + 4\tau)Z(\tau)$ with $t = 1$.

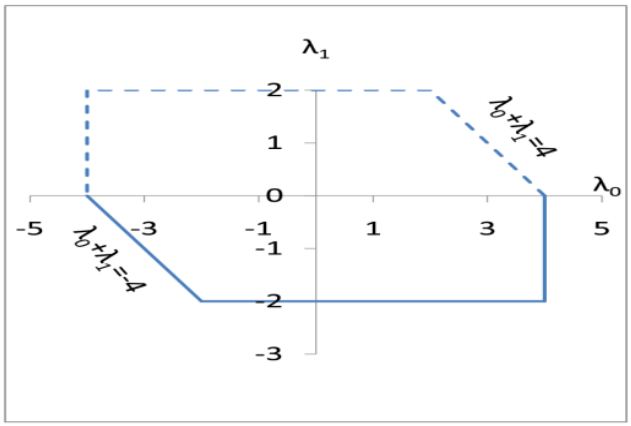

Figure 1: A Voronoi Region of $(-2+4\tau)Z(\tau)$ with $t = 1$.

In the above figure, the division of every element in $\{0,1,2,\dots,27\}$ by $-2+4\tau$ produces $(0,0),(1,0),(2,0),(3,0)$, $(-2,-2),(-1,-2),(0,-2),(1,-2)$, $(2,-2),(3,-2),(4,-2),(-3,0)$, $(-2,0),(-1,0),(0,0)$, $(1,0),(2,0),(3,0),(-2,-2)$, $(-1,-2)$, $(0,-2),(1,-2),(2,-2),(3,-2)$, $(4,-2),(-3,0),(-2,0)$ and $(-1,0)$ respectively. That is, there exist 14 distinct lattice points with 14 pairs of the same points that satisfy the region V. In this case, the number of this distinct points is a total of $2N(-1+2\tau) = 14$ (i.e. supposed to be $N(\psi) = 28$ by Proposition 75 of Solinas, 2000. The actual points in the above figure have been produced from the reduction of $\{0,1,2,\dots,13\}\ mod\ (-2+4\tau)$. Its shows us that the Proposition 75 of Solinas, 2000, is not applicable for the case of $\psi = 2\frac{\tau^3-1}{\tau-1}$. Now, we observing another case by studying first the property of $r+s\tau$.

Theorem 2. Suppose that $r+s\tau = \rho'(r'+s'\tau)$ where $\rho' \in Z$ and $r'+s'\tau \in Z(\tau)$ then $Z \cap (r+s\tau)Z(\tau) = \rho' N(r'+s'\tau)Z$.

Proof.

Let $r+s\tau = \rho'(r'+s'\tau)$, then we obtain

$$Z \cap (r+s\tau)Z(\tau) = Z \cap \rho'(r'+s'\tau)$$
$$\{\dots,-2(r'+s'\overline{\tau}),-(r'+s'\overline{\tau}),0,r'+s'\overline{\tau},2(r'+s'\overline{\tau}),\dots,(i+j\tau)(r'+s'\overline{\tau}),\dots \mid i,j \in Z\}$$

$$= Z \cap \rho' N(r' + s'\tau)\{\dots, -2, -1, 0, 1, 2, \dots, i + j\tau, \dots \mid i, j \in Z\}$$
$$= Z \cap \rho' N(r' + s'\tau)\{Z \cup Z(\tau)\}$$
$$= \rho' N(r' + s'\tau)Z. \quad \blacksquare$$

As a result, the number of lattice points in the interior of Voronoi derived from the division of each element in $\{0,1,2,\dots, N(r+s\tau)-1\}$ by $r+s\tau$ can be obtained by the following corollary.

Corollary 1. Let Voronoi region V is define as Definition 6 and $\psi = r + s\tau$ an element of Z(τ). The number of lattice points in V can be obtained from formula $|\rho'|\, N(r' + s'\tau)$ such that $r + s\tau = \rho'\,(r' + s'\tau)$ where $\rho' \in Z$ and $r' + s'\tau \in Z(\tau)$.

Proof.

Let $r + s\tau = \rho'\,(r' + s'\tau)$ where $\rho' \in Z$ and $r' + s'\tau \in Z(\tau)$. Since $Z \cap (r + s\tau)Z(\tau) = \rho' N(r' + s'\tau)Z$ from Theorem 2, then the number of lattice points in V can be obtained from $|\rho'|\, N(r' + s'\tau)$. ■

For the case that $\psi = \rho\,\frac{\tau^m - 1}{\tau - 1}$, this expression needs to be converted into $r + s\tau$ via Lucas sequence before factoring ψ into $\rho'\,(r' + s'\tau)$. Refer Figure 1, $r + s\tau = -2 + 4\tau$ can be factorized into $2(-1 + 2\tau)$. Hence, $Z \cap (-2 + 4\tau)\, Z(\tau) = 2N(-1 + 2\tau)Z = 14Z$ where the coefficient of Z which is 14 is the number of points in the interior of Voronoi region of $(-2 + 4\tau)Z(\tau)$. The following is an algorithm for obtaining the number of lattice points in the region V of $(r + s\tau)Z(\tau)$, which uses Corollary 1. $N(P_u)$ in the following algorithm is the norm for every lattice points in the Voronoi region. They must be less than or equal to $\frac{4}{7}N(r + s\tau)$ so that the scalar multiplication will not approaches to infinity.

Algorithm 1. (Finding all points in mod $(r + s\tau)$)

Input: Integers r, s, ρ', r' and s' such that $r + s\tau = \rho'\,(r' + s'\tau)$.
Output: All points $x_u + y_u\tau \in mod\ (r + s\tau)$ and their norms respectively.
Computation:

(1) $N(r' + s'\tau) \leftarrow (r')^2 + tr's' + 2(s')^2$.
(2) $N' \leftarrow |\rho'|\, N(r' + s'\tau)$.
(3) For u from 0 to $N' - 1$ do
$k \leftarrow r'u + ts'u.$

$l \leftarrow -s'u.$
$h \leftarrow (r')^2 + tr's' + 2(s')^2.$
$\lambda_0 \leftarrow \frac{k}{h}.$
$\lambda_1 \leftarrow \frac{l}{h}.$

Use Algorithm 3.63 of Hankerso, 2004, for rounding of w and z in $Q(\tau)$ to get elements in $Z(\tau)$.

$x_u \leftarrow u - r'w + 2s'z.$
$y_u \leftarrow -s'w - r'z - ts'z.$
$P_u \leftarrow x_u + y_u\tau.$
$N(P_u) \leftarrow x_u^2 + tx_uy_u + 2y_u^2.$

(4) Return $(P_u, N(P_u))$.

The programming of Algorithm 1 using Maple 13 is shown in the Diagram 1 in Appendix. Once all elements in mod $\rho\frac{\tau^m-1}{\tau-1}$ are known via Algorithm 1, so now it is easy to get the pseudoTNAF expansion for each element. The algorithm is presented in the next section.

5. DENSITY FOR SOME ELEMENTS IN MODULO $\rho\ \frac{\tau^m-1}{\tau-1}$

In this section, we discuss a method for obtaining the density of some elements in mod $\rho\ \frac{\tau^m-1}{\tau-1}$. Firstly, we find the Hamming weight of pseudoTNAF expansions together with their lengths. After that, we calculate the density of each element by dividing the Hamming weight by its length. This density are very important to determine the operating costs of elliptic scalar multiplication with the multiplier for P is based on pseudoTNAF. We developed the following algorithm to obtain all pseudoTNAF for all elements in $\rho\ \frac{\tau^m-1}{\tau-1}$.

Algoritma 2.

Input: Integers x_u, y_u for $u \in \{0,1,2,\dots,N'-1\}$
Output: pseudoTNAF $(x_u + y_u\tau)$
Computation:

$(c_0, c_1) \leftarrow (x_0, y_0)$
$pseudoTNAF_0 \leftarrow 0$
For u from 1 to $N'-1$ do

$(c_0, c_1) \leftarrow (x_u, y_u)$
$i \leftarrow 0$
While $c_0 \neq 0$ or $c_1 \neq 0$ do
    If c_0 is odd then
        $v_i \leftarrow 2 - (c_0 - 2\, c_1 \bmod 4)$
        $c_0 \leftarrow c_0 - v_i$
    else
        $v_i \leftarrow 0$
Endwhile
$R \leftarrow c_0$
$(c_0, c_1) \leftarrow (c_1 + \frac{t \cdot c_0}{2}, -\frac{R}{2})$
$i \leftarrow i + 1$
$j \leftarrow i$
Output $pseudoTNAF_u(v_0, v_2, \ldots, v_{j-1})$

The programming of Algorithm 2 using Maple 13 is shown in the Diagram 2 in Appendix. Through the above algorithm, the number of bits of N' can be used as a guide to find an integer u which is a multiplier of scalar multiplication. For example, if $a = 0$, $\rho_0 = 1$, $\rho_1 = -1$ and $m = 163$, then $N' = 1169201309864722334562947381626363161783 6683539492$.

The maximum number of bits available for integer u in mod (-333474650358695802588112 9- 1824026374634505274957943 τ) is about 163 bits. In other words, we can get all integers u with their sizes between 1 to 163 bits. The question now, does all integers u from 1 to $N' - 1$ suitable to be used as the multipliers for scalar multiplication? According to Solinas, 2000, the sizes of the practical multiplier for ECC is between 96 to 128 bits for $m = 163$. It is not necessary to examine all points u from 1 to $N' - 1$.That is, the integers u should be in element of [396140812571321687967719751 68,340282366920938463463374607431768211455].

That means, there are 340282366881324382206242438634996236288 choice of multipliers that might be used in the scalar multiplication. Several options u can be made randomly by doing part by part looping. For example, to obtain the pseudoTNAF for u in Table 1, the command ' for u from 0 to $N' - 1$ do' and 'for u from 1 to $N' - 1$ do' can be replaced by the command 'for u from 792281625142643375935439503 35 to 7922816251426433759 3543950339 do'.

TABLE 1: Density of pseudoTNAF for some integers u modulo $(1-\tau)\frac{\tau^{163}-1}{\tau-1}$ with their sizes are 96 and 97 bits

u	Size of bits	Length of pseudoTNAF	Hamming weight	Density (5decimal places)
792281625142643375935439503 35	96	157	29	0.18471
792281625142643375935439503 38	96	157	28	0.17834
792281625142643375935439503 36	97	157	30	0.19108
792281625142643375935439503 37	97	157	29	0.18471
792281625142643375935439503 39	97	157	27	0.17197

From the above table, the average Hamming weight among integer u of length 157 is $\frac{29+28+30+29+27}{5}=28.6$. This value is equal to $\frac{0.18471+0.17834+0.19108+0.18471+0.171}{5}=0.182162$, the average density among integer u of length 157) multiplied by the length 157. With a few multiplier u that randomly chosen will not be able to give an estimation of the actual average Hamming weight of pseudoTNAF with maximum length. The question remains how such estimation can be made? This will be discussed in detail in the next topic.

6. AVERAGE HAMMING WEIGHT AMONG PSEUDOTNAF OF MAXIMUM LENGTH

Gordon, 1998, has shown that the average Hamming weight of TNAF of all length m integers of $[1, N(\tau^m-1)-1]$ is approximately $\frac{m}{3}(1+o(1))$ when $m\to\infty$. This estimation is a product of multiplying the average density $\frac{1}{3}+o(1)$ with the maximum length (i.e. m). By taking the same average density, Solinas, 2000, has shown that the average Hamming weight of RTNAF of all length $m+a$ integers of $[1, N(\frac{\tau^m-1}{\tau-1})-1]$ is about $\frac{m}{3}$ when $m\to\infty$. Such average is a product of multiplying the average density $\frac{1}{3}+o(1)$ with the maximum length (i.e. $m+a$). Now, our study provides an estimation of average density of pseudoTNAF via the following proposition. The average is estimated to be equal to $\frac{1}{3}+o(1)$ as Gordon, 1998, with some modifications against the arguments given by him.

Proposition 2. The average density of pseudoTNAF is approximately $\frac{1}{3}+o(1)$.

Proof.

Integer reduction of $\{0,1,\dots,|\rho'|\,N(r'+s'\tau)-1\}$ cover all congruence classes modulo $\rho(\frac{\tau^m-1}{\tau-1})$. Integer $|\rho'|\,N(r'+s'\tau)$ is the number of lattice points in the Voronoi region of $\rho N(\frac{\tau^m-1}{\tau-1})Z(\tau)$ as in Corollary 1. Every integers of $\{0,1,\dots,|\rho'|\,N(r'+s'\tau)-1\}$ are divided by $\rho(\frac{\tau^m-1}{\tau-1})$ to get a total of $|\rho'|\,N(r'+s'\tau)$ lattice points that can be obtained through the Algorithm 1. Each lattice points of length $\bar{l}$ are complete distributed to some Voronoi region of $\tau^{\bar{l}+3}\,Z\,(\tau)$ that overlaps with the Voronoi region of $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$. Then, pseudoTNAF of each points obtained from the Algorithm 2. The number of pseudoTNAF of $\bar{l}>2$ is greater than 4 and less than $N(\tau^{\bar{l}+3})$. Thus, the average density of the maximum length can be identified and it is approximately $\frac{1}{3}+o(1)$. ■

Finally, the average Hamming weight among pseudoTNAF of maximum length can be estimated. This is explained in the following theorem.

Theorem 2. The average Hamming weight among pseudoTNAF of all integers modulo $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$ with maximum length is approximately $\left(\frac{1}{3}+o\,(1)\right)(log_2\,N(\rho)+m+a)$.

Proof.

The maximum length of the pseudoTNAF expansion can be obtained from Theorem 2.7 of Yunos et al., 2014, i.e. $log_2\,N(\rho)+m+a$. Whereas the average density of pseudoTNAF is around $\frac{1}{3}+o\,(1)$ obtained from Proposition 2. Therefore, The average Hamming weight is

$$\left(\tfrac{1}{3}+\,o\,(1)\right)(log_2\,N(\rho)+m+a).\ ■$$

7. CONCLUSION

Proposition 1 has proved that pseudoTNAF is equivalent to TNAF in set $E_a\ (F_{2^m})$. Therefore, the pseudoTNAF can be used as a multiplier to the scalar multiplication with condition (3) so that scalar multiplication is not towards to infinity. Now, the operational costs when using pseudoTNAF can be estimated via the average Hamming weight of pseudoTNAF. That is approximately $\left(\frac{1}{3} + o\,(1)\right)(log_2\, N(\rho) + m + a)$.

We also developed one algorithm for finding all pseudoTNAF in modulo $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$. Retrieval from this algorithm is important to get the lowest operational costs of scalar multiplication for a certain ρ and m that will be the subject of our future discussion.

REFERENCES

Avanzi, R. M., Heuberger, C. and Prodinger, H. (2005). *Minimality of the Hamming Weight of the τ-NAF for Koblitz Curves and Improved Combination with Point Halving*. http://eprint.iacr.org/2005/ 225.pdf

Brumley, B.B. and Jarvinen, K. (2007). Koblitz Curves and Integer Equivalents of Frobenius Expansions. *Lecturer Notes in Computer Science*. **4876**: 126-137. Springer.

Gordon, D.M. (1998). A Survey of Fast Exponentiation Methods. *Journal of Algorithms 27, Article no* ***AL970913***, 129-146.

Hankerson, D., Menezes, A., and Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. Springer-Verlag.

Hakuta, K., Sato, H. and Takagi, T. (2010). Explicit Lower bound for the Length of Minimal Weight τ-adic Expansions on Koblitz Curves. *Journal of Math-for-Industry.* **2** (2010A-7): 75-83.

Joye, M. and Tymen, C. (2001). Protection against Differential Analysis for Elliptic Curve Cryptography: An Algebraic Approach, in *Cryptography Hardware and Embedded Systems-CHES'***01**, *Lecturer Notes in Computer Science.* **2162**:377-390. Springer-Verlag.

Koblitz, N. (1987). Elliptic curve cryptosystem, *in Mathematics Computation*. **48** (177): 203-209.

Koblitz, N. (1992). CM curves with good cryptographic properties. *Proc. Crypto*'**91**: 279-287. Springer-Verlag.

Li, M., Qin, B., Kong, F. and Li, D. (2007)**.** Wide-W-NAF Method for Scalar Multiplication on Koblitz Curves. *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/ Distributed Computing*: 143-148.

Lin, T. C. (2009). Algorithm on Elliptic Curves over fields of Characteristic Two with Non-Adjacent Forms. *International Journal of Network Security*. **9**(2): 117-120.

Ratsimihah, J.R. and Prodinger, H. (2005). *Redundant Representation of Numbers*. *http://resources.aims.ac.za/archive/2005/joel.ps*

Roy, S. S., Robeiro, C., Mukhopadhyay, D., Takahashi, J. and Fukunaga, T. (2011). *Scalar Multiplication on Koblitz Curves Using* τ^2 *-NAF*. http://eprint.iacr.org/2011/318.pdf

Solinas, J. A. (1997). An Improved Algorithm for Arithmetic on a Family of Elliptic Curves, in B. Kaliski, editor, *Advance in Cryptology-CRYPTO*'**97**. *Lecture Notes in Computer Science*. **1294**: 357-371. Springer-Verlag.

Solinas, J. A. (2000). Efficient Arithmetic on Koblitz Curves, in Kluwer Academic Publishers, Boston, Manufactured in the Netherlands, *Design, Codes, and Cryptography*. **19**:195-249.

Yunos, F. and Mohd Atan, K. A. (2013). An Average Density of τ-adic Naf (τ -NAF) Representation: An Alternative Proof. *Malaysian Journal of Mathematical Sciences*. **7(1)**: 111 - 124.

Yunos, F., Mohd Atan, K. A., Md. Said, M. R. and Kamel Ariffin, M. R . (2014). A Reduced τ -NAF **(**RTNAF) Representation for Scalar Multiplication on Anomalous Binary Curves (ABC). *Pertanika Journal of Science and Technology*. **22(2**): 125-141.

APPENDIX

$r := any\ integer$; $s := any\ integer$; $a :=$ 0 or 1; $t = (-1)^{1-a}$;
$F := gcd(r, s)$; $\#F$ is ρ'
$G := \frac{r}{F}$; $H := \frac{s}{F}$; $\#G$ is r' and H is s'
$NewN := F \cdot (G^2 + t \cdot G \cdot H + 2 \cdot H^2)$; $\#NewN$ is N'
for u from 0 to $NewN - 1$ do
$k := r \cdot u + t \cdot s \cdot u$; $l := -s \cdot u$; $h := r^2 + t \cdot r \cdot s + 2 \cdot s^2$;
$\lambda_0 := \frac{k}{h}$; $\lambda_1 := \frac{l}{h}$;
for i from 0 to 1 do
$f_i := floor\left(\lambda_i + \frac{1}{2}\right)$;
$\eta_i := \lambda_i - f_i$; $h_i := 0$;
end do;
$\eta_2 := 2 \cdot \eta_0 + t \cdot \eta_1$;
$\Omega_0 := \eta_2 \geq 1$; $evalb(\Omega_0)$;
$\Omega_1 := (\eta_0 - 3 \cdot t \cdot \eta_1) < -1$; $evalb(\Omega_1)$;
$\Omega_2 := (\eta_0 + 4 \cdot t \cdot \eta_1) \geq 2$; $evalb(\Omega_2)$;
$\Omega_3 := (\eta_0 - 3 \cdot t \cdot \eta_1) \geq 1$; $evalb(\Omega_3)$;
$\Omega_4 := (\eta_0 + 4 \cdot t \cdot \eta_1) < -2$; $evalb(\Omega_4)$;
$\Omega_5 := \eta_2 < -1$; $evalb(\Omega_5)$;
if Ω_0 then
if Ω_1 then $h_1 := t$;
else $h_0 := 1$;
end if;
else
if Ω_2 then $h_1 := t$;
end if;
end if;
if Ω_5 then
if Ω_3 then $h_1 := -t$;
else $h_0 := -1$;
end if;
else
if Ω_4 then $h_1 := -t$
end if;
end if;
$w := f_0 + h_0$; $z := f_1 + h_1$;
$x_u := u - r \cdot w + 2 \cdot s \cdot z$; $y_u := -s \cdot w - r \cdot z - t \cdot s \cdot z$;
$P_u := x_u + y_u \cdot \tau$;
$N[P_u] := x_u^2 + t \cdot x_u \cdot y_u + 2 \cdot y_u^2$;
end do;
$AllPoints := seq(O_u = P_u, u = 0 \,..\, NewN - 1)$;
$NormForEveryPoints := seq(Norm[O_u] = N[P_u], u = 0 \,..\, NewN - 1)$;

#Find x_u and y_u using Diagram 1 for u from 0 to $NewN - 1$.
$c_0 := x_0;\ c_1 := y_0;\ pseudoTNAF_0 := 0;\ LengthpseudoTNAF_0 := 1;$
$HammingWeight_0 := 0; Density_0 := 0;$
for u from 1 to $NewN - 1$ do
$c_0 := x_u;\ c_1 := y_u;\ i := 0;$
while $c_0 <> 0$ or $c_1 <> 0$ do
$o := type(c_0, odd);\ evalb(o);$
$if\ o\ then$
$f := c_0 - 2 \cdot c_1;$
$d := convert(f, rational);$
$e := modp(d, 4);$
$v_i := 2 - e;$
$c_0 := c_0 - v_i;$
else
$v_i := 0;$
end if;
$R := c_0;$
$c_0 := c_1 + \frac{t \cdot c_0}{2};$
$c_1 := -\frac{R}{2};$
$i := i + 1;$
$j := i;$
end do;
$pseudoTNAF_u := [seq(v_i, i = 0..j - 1)];$

Diagram 1: The Programming of Algorithm 1 using Maple 13