Malaysian Journal of Science 37 (2): 94 – 102 (2018)

EVEN AND ODD NATURE FOR PSEUDO τ-ADIC NON-ADJACENT FORM

Faridah Yunos[a,*] **, Syahirah Mohd Suberi**[b]

[ab] Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor, 43400, Malaysia.
[a] Department of Mathematics, Universiti Putra Malaysia, Serdang, Selangor, 43400, Malaysia.
[*]Correspondence Author: faridahy@upm.edu.my
Received: 7th March 2017 Revised: 18th October 2018 Accepted: 12th December 2018
DOI: https://doi.org/10.22452/mjs.vol37no2.2

ABSTRACT An algorithm was developed by previous researcher for elliptic scalar multiplication (SM) on Koblitz curve where the multiplier of SM is in the form of Pseudo τ-adic Non-Adjacent (pseudoTNAF). PseudoTNAF of $i + j\tau$ an element of the ring $\mathrm{Z}(\tau)$ where $i, j \in \mathrm{Z}$ is an expansion where the digits are generated by successively dividing $i + j\tau$ by τ, allowing remainders of -1, 0 or 1. Such a multiplier is in the form of $i + j\tau \equiv n \bmod (r_0 + r_1\tau)\left(\frac{\tau^m - 1}{\tau - 1}\right)$. In this paper, we refine some properties of the multiplier $r_0 + r_1\tau$ from previous researchers focusing on even and odd situation for r_0 and r_1. We also propose two properties of $r_0 + r_1\tau$ when r_0 is even and r_1 is odd. As a result, the nature of $i - n$ and j are depends on the nature of r_0 and r_1 when r_0 is even. Whereas, the nature of $i - n$ and j are not depends on the nature of r_0 and r_1 when r_0 is odd.

Keywords: Pseudo τ-adic Non-Adjacent Form (pseudoTNAF); scalar multiplication (SM); Koblitz curve

INTRODUCTION

Elliptic curve cryptography is an approach to public-key cryptography based on the algebraic structure of Elliptic Curve (EC) over finite field. This system was standardized as the most secured system in information security. The generation of F_{2^m} as

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

where a an element of {0,1} and $P = (x, y)$ on the curve (Koblitz (1987)). The Frobenius map

$$\tau: E_a(F_{2^m}) \to E_a(F_{2^m})$$

is defined by

$$\tau(x, y) = (x^2, y^2), \tau(\infty) = \infty$$

domain parameters is not usually done by previous researchers because this involves computing SM for an integer n and a point P on EC which is time-consuming and complex to implement. The Koblitz curves are special types of curves for which the Frobenius endomorphism can be used for improving the performance of computing an elliptic SM (Koblitz (1992)). It is defined over where ∞ is the point at infinity. The imaginary quadratic number $\tau = \frac{t + \sqrt{-7}}{2}$ satisfies the relation $\tau^2 - t\tau + 2 = 0$ where $t = (-1)^{1-a}$. Figure 1 is an illustration of the SM in this set (Yunos et al. , 2015).

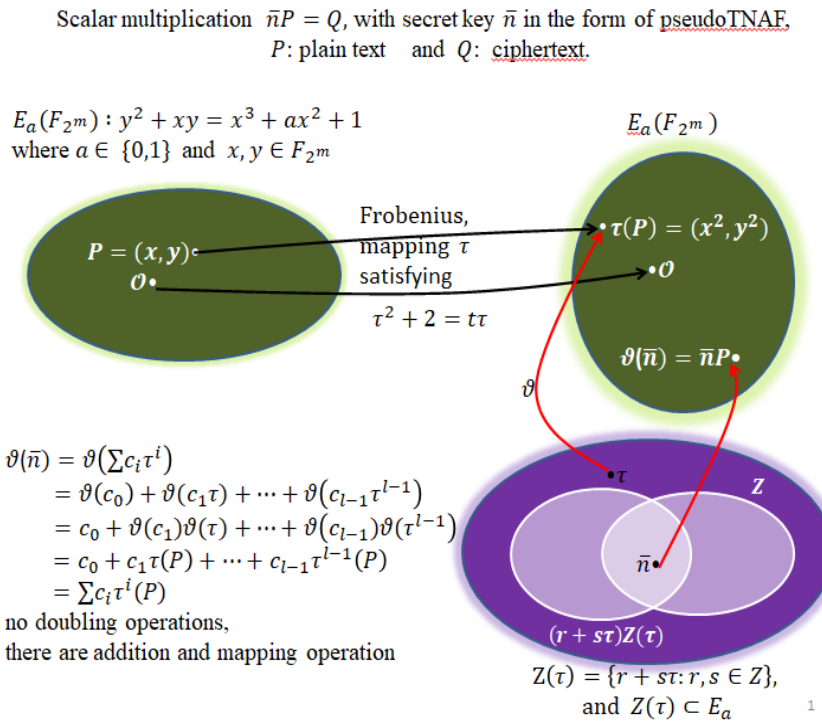

Figure 1- An illustration of the SM on the set $E_a(F_{2^m})$.

In the literature, there are two methods used to express all elements (x, y) which are either in the form of polynomial basis or normal basis. Whereas, FIPS PUB 186-4 gives the bit sizes range of the order for basis point (x, y) in the binary field of sizes 163, 233, 283, 409 and 571, together with the list of some suitable parameters for five types of Koblitz curves. This information is the standard proposed by FIPS PUB 186-4 and can be referred to Kerry and Gallagher (2013). This is the fourth series of publications with expertise and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA).

The following are some definitions and lemma can be found in Solinas (2000); Heuberger and Krenn (2012); Yunos et al. (2014); Yunos et al. (2015a); Yunos et al. (2015b); Yunos and Mohd Atan (2016); Mohd Suberi et al. (2016); Ali and Yunos (2016) that will be used throughout this study.

Definition 1. $Z(\tau)$ is the set of polynomials in τ. Defined $Z(\tau)$ to be quotient ring

$$Z(x)/(x^2 - tx + 2^m) .$$

Lemma 1. (Heuberger and Krenn (2012)) If τ is quadratic then $(\tau) = \{ r + s\tau : r, s \in Z\}$.

Definition 2. A τ-adic non-adjacent form (also called τ-NAF or TNAF) of nonzero $\bar{n}$ in $Z(\tau)$ is equal to $\sum_{i=0}^{l-1} c_i \tau^i$ where $c_i \in \{-1, 0, 1\}$ and $c_i c_{i+1} = 0$ for all i. If $c_{l-1} \neq 0$ then l is said to be the length of τ-NAF.

TNAF($\bar{n}$) in the form of $\sum_{i=0}^{l-1} c_i \tau^i$ is an expansion where the digits are generated by successively dividing $\bar{n}$ by τ, allowing remainders $-1, 0$ or 1.

Definition 3. A Reduced τ-adic Non-Adjacent Form (also called RTNAF) of nonzero $\bar{n}$ in $Z(\tau)$ is $\sum_{i=0}^{l-1} c_i \tau^i$ that is equal to n mod $\frac{\tau^m-1}{\tau-1}$, and where $c_i \in \{-1, 0, 1\}$ and $c_i c_{i+1} = 0$ for all i. If $c_{l-1} \neq 0$ then l is said to be the length of RNAF.

Definition 4. A Pseudo τ-adic Non-Adjacent Form (also called pseudoTNAF) of nonzero $\bar{n}$ in $Z(\tau)$ is $\sum_{i=0}^{l-1} c_i \tau^i$ that is equal to n mod $\left(\frac{\tau^m-1}{\tau-1}\right)$, and where $\rho \in Z(\tau)$, $c_i \in \{-1, 0, 1\}$ and $c_i c_{i+1} = 0$ for all i. If $c_{l-1} \neq 0$ then l is said to be the length of pseudoTNAF.

Definition 5. Let $N : \mathbb{Q}(\tau) \to \mathbb{Q}$ the rational set as a function of norm. Let $\alpha = x + y\tau$ an element $\mathbb{Q}(\tau)$. The norm of α is $N(\alpha) = x^2 + txy + 2y^2$ where $t = (-1)^{(1-a)}$ and $a \in \{0, 1\}$.

$\frac{\tau^m-1}{\tau-1}$ and $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$ in Definitions of 3 and 4 respectively can be converted into $r + s\tau$. We choose any integer n from interval [1, $|p'|N(r' + s'\tau) - 1$] such that $r + s\tau = p'(r' + s'\tau)$ where p' is an integer. After that, $\bar{n}$ in $Z(\tau)$ can be generated from dividing an integer n by $r + s\tau$. Lastly, the RTNAF($\bar{n}$) and pseudoTNAF($\bar{n}$) in the form of $\sum_{i=0}^{l-1} c_i \tau^i$ are expansions where the digits are generated by successively dividing $\bar{n}$ by τ, allowing remainders $-1, 0$ or 1.

Definition 6. Let P and Q be the point on Koblitz curve for $P = (x, y)$. Scalar multiplication is the repeated addition of a point along the curve up to n times and denoted as $nP = P + P + \cdots + P$ for some scalar n such that $nP = Q$.

Definition 7. Lucas sequence are defined as

$$U_0 = 0, U_1 = 1 \text{ and}$$
$$U_i = tU_{i-1} - 2U_{i-2} \text{ for } \quad i \geq 2.$$

In this paper, we gather all the properties for $r_0 + r_1\tau$ in $i + j\tau \equiv n \, mod \, (r_0 + r_1\tau)\left(\frac{\tau^m-1}{\tau-1}\right)$. In Section 2, we give the previous study developed by some earlier researchers. Next, in Section 3, we begin with restating all the seventh properties r_0 and r_1 involving an even and odd situation that have been proposed by Yunos et al. (2014) and Mohd Suberi et al. (2016). We introduced two properties of such r_0 and r_1. These all nine properties will help us to understand the nature of i and j when using $i + j\tau \equiv n \, mod \, (r_0 + r_1\tau)\left(\frac{\tau^m-1}{\tau-1}\right)$.

LITERATURE REVIEW

Solinas (1997) was mention that the Hamming weight of non-adjacent form (NAF) of integer n satisfies $\approx \frac{1}{3}\log_2 n$. Therefore, the average cost using addition–subtraction method is $\sim m$ doubles and $\sim \frac{m}{3}$ additions, for a total of $\sim \frac{4m}{3}$ elliptic operations. He improved this method by introducing the expression n in $Z(\tau)$ of the form τ-adic non-adjacent (TNAF). That is, the digits of expansions of n are generated by successively dividing n by τ, allowing remainders of $-1, 0$ and 1. The average Hamming weight of the TNAF for the integer n satisfies $\approx \frac{2}{3}\log_2 n$. This is twice as large as the Hamming weight of an ordinary NAF. Replacing the ordinary NAF by TNAF will eliminate the elliptic doublings and double the number of elliptic additions. The algorithm developed by him is one of the most efficient algorithms to compute the SM on Koblitz curve. The average number of elliptic operation is $\sim \frac{m}{3}$. Solinas (2000) was able to maintain this situation by replacing an integer n in the form of TNAF with an expansion in the form of reduced TNAF (RTNAF). The reduction concept in the field of rational integer has been discussed by Solinas (2000). To avoid SM towards to infinity, the residue n mod $(r+s\tau)$ must have a norm as small as possible i.e. $N(n)$ is less than or equal to $\frac{4}{7}N(r+s\tau)$. An algorithm for division in Z(τ) (i.e. the polynomial ring in Z(τ)) with integer coefficients) in Solinas (1997) provides detail reduction steps for n mod $(r + s\,\tau)$. This algorithm has been used by Solinas (2000) in the reduction of n mod $\frac{\tau^m-1}{\tau-1}$. Since the average Hamming weight among reduced TNAF is $\sim \frac{m}{3}$. Replacing TNAF by reduced TNAF can reduced the length of expansion of n about half as long. Since the Hamming weight of TNAF is $\approx \frac{2}{3}\log_2 n$, then the reduced TNAF has about half the weight of TNAF. Since, the

Hamming weight of NAF satisfies $\approx \frac{1}{3}\log_2 n$ then the Hamming weight of reduced TNAF is about equal to that of NAF. Thus, replacing NAF by reduced TNAF eliminates the elliptic doubles and keeps roughly constant the number of elliptic addition. Reduced TNAF can be used in place of TNAF. The properties of n mod $(r + s\,\tau)$ for SM on different types of curves have also been developed by some researchers such as Avanzi et al. (2007); Blake et al. (2008); Avanzi et al. (2010); Heuberger (2010); Hakuta et al. (2010); Karthikeyan et al. (2011); Heuberger and Krenn (2011, 2012); Yunos et al. (2014); Yunos et al. (2015a, 2015b); Yunos and Mohd Atan (2016), Mohd Suberi et al. (2016, 2018); Ali and Yunos (2016) and Ali et al. (2017).

Pseudo τ-adic Non-adjacent Form (pseudoTNAF) of $\bar{n}$ where $\bar{n} \equiv n \bmod (r_0 + r_1\tau)\frac{\tau^m-1}{\tau-1}$ for SM on Koblitz Curve was developed by Yunos et al. (2014). It has been proven that pseudoTNAF equivalent to the TNAF and RTNAF. Reducing the operating cost of the SM by using pseudoTNAF for an element in Z(τ) can eliminate the elliptic doublings in the SM method on Koblitz curve, and double the number of elliptic additions. This is due to the costs for implementing the Frobenius map τ is basically free. Therefore, the cost only depends on the average of the number of non-zero coefficients among pseudoTNAF's expansion. To make the reduction of n become easier, Yunos et al. (2014) implement Lucas sequence in transforming element from $(r_0 + r_1\tau)\frac{\tau^m-1}{\tau-1}$ to $r + s\,\tau$. Yunos et al. (2015a) proved that the number of distinct points in mod $(r + s\,\tau)$ can be obtained from formula $|p'|N(r' + s'\,\tau)$ such that $r + s\tau = p'(r' + s'\tau)$ where p' is an integer. This is reinforced with Proposition 75 in Solinas (1997) which stated that the formula is exactly N($r + s\tau$). Combining the condition of N(n) with this guideline, Yunos et al. (2015a) proposed an algorithm for finding all points in mod $r + s\tau$. As a result, the estimation cost of carrying out the pseudoTNAF method is about $\left(\frac{1}{3} + o(1)\right)(log_2 N(r_0 + r_1\tau) + m + a)$ number of additions. This estimation cost based on average density of the Hamming weights of expansion. Each hamming weight gives one additional in cost calculation. It was described in Yunos et al. (2016) which was referred to Table 1 which gives the comparison of expansion length (l), the number of Hamming weight (HW) and the density of pseudoTNAF($\bar{n}$) for $n = 79228162514264337593549503 50$, $a = 0$, $m = 163$, with different $r_0 + r_1\tau$.

Table 1- Comparison of Density for Different Type of $r_0 + r_1\tau$

The type of expansion	l	HW	Density
$\bar{n} \equiv n \bmod (2+\tau)\frac{\tau^{163}-1}{\tau-1}$	163	53	0.32515
$\bar{n} \equiv n \bmod 4\frac{\tau^{163}-1}{\tau-1}$	164	28	0.17073
$\bar{n} \equiv n \bmod (1-\tau)\frac{\tau^{163}-1}{\tau-1}$	157	28	0.17834
$\bar{n} \equiv n \bmod \frac{\tau^{163}-1}{\tau-1}$	157	28	0.17834
$\bar{n} \equiv n \bmod (\tau-1)\frac{\tau^{163}-1}{\tau-1}$	157	28	0.17834

From Table 1, there is sometime the density value of pseudoTNAF($\bar{n}$) becomes lower or higher or equivalent to RTNAF($\bar{n}$) and TNAF($\bar{n}$). This situation is affected by the value of $r_0 + r_1\tau$. We found that the density of nonzero coefficients in pseudoTNAF expansion is similar to TNAF and RTNAF when $r_0 + r_1\tau = 1 - \tau$. For $r_0 + r_1\tau = 4$, the density of such pseudoTNAF is less four percents than the others although the size of it's expansion a bit longer. Meanwhile, the density becomes higher when $r_0 + r_1\tau = 2 + \tau$. Therefore, the choice of $r_0 + r_1\tau$ is important to reduce the operating cost of scalar multiplication. This method (with an appropriate $r_0 + r_1\tau$) is four percents more effective than the method of selecting TNAF and RTNAF. To estimate this cost more accurately, Ali and Yunos (2016) and Ali et al. (2017) suggested the use of total, maximum and minimum norm formulas for TNAF that was occurring among of all elements in Z(τ). Whereas the selection of seven types of $r_0 + r_1\tau$ involving even and odd situation for r_0 and r_1 as described in Yunos et al. (2014) and Mohd Suberi et al. (2016) should be considered. It can influence any attackers to guess an original message. In this study, we investigate some more properties in the similar

situation. Furthermore, these properties can be scrutinized the effect of choosing $r_0 + r_1\tau$ which is related to the concept of congruence modulo $(r_0 + r_1\tau)\left(\frac{\tau^m-1}{\tau-1}\right)$.

RESULTS AND DISCUSSION

Before we proceed to the new cases of $r_0 + r_1\tau$, we rephrase back the seventh properties that have been developed by Yunos et al. (2014) and Mohd Suberi et al. (2016) as follows.

Theorem 3.10
Let $r_0 + r_1\tau \in Z(\tau)$ and r_0 is even. If $(r_0 + r_1\tau)|(r + s\tau)$, then r is even.

Theorem 3.11
Let $r_0 + r_1\tau \in Z(\tau)$ and r_0 and r_1 are even. If $(r_0 + r_1\tau)|(r + s\tau)$, then r and s are even.

Theorem 3.12 If r_0 is even, r_1, c and d are odd, then $(r_0 + r_1\tau)(c + d\tau) = r + s\tau$ where r and s are even.

Theorem 3.13 If r_0 and d are even, r_1 and c are odd, then $(r_0 + r_1\tau)(c + d\tau) = r + s\tau$ where r is even and s is odd.

Theorem 3.14 If r_0, c and d are odd and r_1 is even, then $(r_0 + r_1\tau)(c + d\tau) = r + s\tau$ where r and s are odd.

Theorem 3.15 If r_0, r_1 and c are odd, then $(r_0 + r_1\tau)(c + d\tau) = r + s\tau$ where r and s are odd.

Theorem 3.16 If r_0 and c are odd and r_1 and d are even, then $(r_0 + r_1\tau)(c + d\tau) = r + s\tau$ where r is odd and s is even.

Now, we proceed with two more properties to complete all possible combination of r_0, r_1, c and d involving *e*ven and odd cases as follows.

Theorem 3.17 If r_0, c and d are even and r_1 is odd, then $(r_0 + r_1\tau)(c + d\tau) = r + s\tau$ where r and s are even.

Proof

This theorem has been proven from Theorem 3.11 since the multiplication of elements in Z(τ) satisfied the commutativity property.

Theorem 3.18 If r_0 and c are even and r_1 and d is odd, then $(r_0 + r_1\tau)(c + d\tau) = r + s\tau$ where r is even and s is odd.

Proof .

Let $r_0 = 2k_1, r_1 = 2k_2 + 1, c = 2l_1$ and $d = 2l_2 + 1$ with $k_1, k_2, l_1, l_2 \in Z$.

$$
\begin{aligned}
&(r_0 + r_1\tau)(c + d\tau)\\
&\quad = (2k_1 + (2k_2 + 1)\tau)(2l_1 + (2l_2 + 1)\tau)\\
&\quad = 4k_1l_1 + 4k_1l_2\tau + 2k_1\tau + 2k_2l_1\tau + 2k_2l_2\tau^2 + 2k_2\tau^2 + 2l_1\tau + 2l_2\tau^2 + \tau^2\\
&\quad = 2(2k_1l_1) + 2(2k_1l_2 + k_1 + k_2l_1 + l_1)\tau + (2k_2l_2 + 2k_2 + 2l_2 + 1)(t\tau - 2)\\
&\quad = 2(2k_1l_1 - 2k_2l_2 - 2k_2 - 2l_2 - 1) + (2(2k_1l_2 + k_1 + k_2l_1 + l_1 + k_2l_2t + k_2t + l_2t) + t)\tau
\end{aligned}
$$

Let $a = 2k_1l_1 - 2k_2l_2 - 2k_2 - 2l_2 - 1$ and $b = 2k_1l_2 + k_1 + k_2l_1 + l_1 + k_2l_2t + k_2t + l_2t$.
Therefore $r = 2a$ which is even and $s = 2b + t$ where t can be either 1 or -1.

As a result, we summarized the outcome of r and s from Theorems 3.10-3.18 with different combinations of r_0, r_1, c and d as in Diagrams 1 and 2. This shows all the possible of r_1, c and d involving even and odd numbers when r_0 is even and r_0 is odd respectively. Whereas r and s are the product for the multiplication $r_0 + r_1\tau$ with $c + d\tau$.

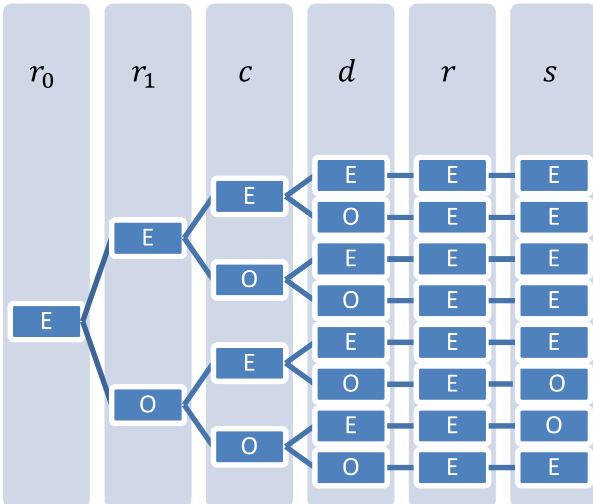

Diagram 1- All combination of r_1, c, d, r and s when r_0 is even

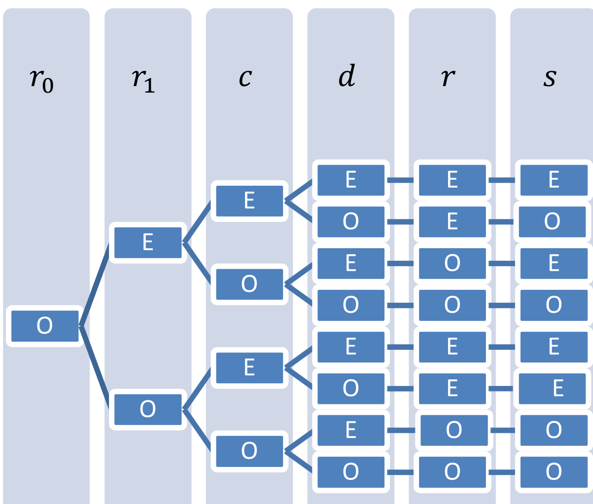

Diagram 2- All combination of r_1, c, d, r and s when r_0 is odd.

From Diagrams 1 and 2, we conclude the result as follows.

1. If r_0 is even, then $(r_0 + r_1\tau)|(r + s\tau)$ where r is even.

2. If both r_0 and r_1 are even, then $(r_0 + r_1\tau)|(r + s\tau)$ where both r and s are also even.

3. If r_0 even and r_1 odd, then $(r_0 + r_1\tau)|(r + s\tau)$ where r is even and s is any integer.

4. In all situation when r_0 is odd, we are not able to guess the nature of r and s such that $(r_0 + r_1\tau)|(r + s\tau)$.

The four situations mentioned above influence the multiplier $i + j\tau$ in a cryptographic system where $i + j\tau \equiv n \bmod (r{+}s\tau)$ especially when $i + j\tau \equiv n\, mod(r_0 + r_1\tau)\left(\frac{\tau^m - 1}{\tau - 1}\right)$. Moreover, the following prediction can be made.

(i) Suppose $(r_0 + r_1\tau)\left(\frac{\tau^m-1}{\tau-1}\right) = r + s\tau$. The nature of r and s are depends on the nature of r_0 and r_1 when r_0 is even.

(ii) The nature of $i - n$ and j are depends on the nature of r_0 and r_1 when r_0 is even. This is an implication of Theorems 3.10-3.13, 3.17 and 3.18.

(iii) The nature of $i - n$ and j are not depends on the nature of r_0 and r_1 when r_0 is odd. This is an implication of Theorems 3.14-3.16.

The description of the argument number (ii) is in the following example.

Example 1.

Consider $r_0 = 0$ and $r_1 = 2$ such that $r{+}s\tau = 2\tau\frac{\tau^3-1}{\tau-1}$. From Theorem 3.10, if r_0 even, then r is even. We can verify that the expression $2\tau\frac{\tau^3-1}{\tau-1}$ is transforms into $-8 + 2\tau$. Let us choose randomly an integer $n = 13$ with 4 bits sizes from an interval $[1,\ 2\,N(-4 + \tau) - 1]$ as the multiplier of scalar multiplication. Now, we have $13\ mod\ -8 + 2\tau$. Integer 13 can be converted to $i + j\tau = 1 - 4\tau$ via division process in $Z(\tau)$. It is proven that $r = -8$ is even then $i - n = -12$ is also even from Theorem 3.10. Dividing $1 - 4\tau$ by τ produces pseudoTNAF$(1 - 4\tau)$ is equals $[1,0,0,-1,0,0,-1] = 1 - \tau^3 - \tau^6$ (refer this calculation in Appendix A). We found that the first coefficient for this expansion is beginning with 1 and after that is 0. This pattern refers to Proposition A2 in Appendix A (Yunos et al. (2018). We can

take advantage from this proposition that $i + j\tau = 1 - 4\tau$ is follows the pattern of $5 + 4k$ where the first coefficient of pseudoTNAF$(1 - 4\tau)$ is 1. In this example the exact values of i and j are easily can be found because we know the n is equal to 13. Moreover, the norm of $-8 + 2\tau$ is small and therefore we can guess the exact values of i and j by using Algorithms 4.2 or 4.3 in Yunos et al. (2015b).

CONCLUSION

From Theorems 3.10-3.18, we conclude that the nature of $i - n$ and j in $i + j\tau \equiv n \, mod \, (r_0 + r_1\tau)\frac{\tau^m - 1}{\tau - 1}$ are depends on the nature of r_0 and r_1 when r_0 is even. Whereas, the nature of $i - n$ and j are not depends on the nature of r_0 and r_1 when r_0 is odd. The chosen of r_0 when it is even should be carefully considered for cryptographic proposes for the system that uses pseudoTNAF expansion especially when the norm of $(r_0 + r_1\tau)\left(\frac{\tau^m - 1}{\tau - 1}\right)$ is small.

REFERENCE

Ali, N.A. and Yunos, F. (2016). Maximum and Minimum Norms for τ-NAF Expansion on Koblitz Curve. Indian Journal of Science and Technology, Vol 9(28):1-7.

Ali, N.A. and Yunos, F., Jamal, N.H. (2017). A Total norm of τ -adic Non-Adjacent Form Occuring among all Element of Z(τ): An Alternative Formula. In the 2nd International Conference and Workshop on Mathematical Analysis (ICWOMA2016). AIP Publishing, Vol 1795. p. 020002.

Avanzi, R.M., Heuberger, C. and Prodinger, H. (2007). On Redundant T-adic Expansions and Non-Adjacent Digit Sets. In Proceeding of the 13th International Workshop on Selected Area in Cryptography, SAC 2006, 285-301. Springer Verlag.

Avanzi, R. M., Heuberger, C. and Prodinger, H. (2010). http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.370.9584.

Blake, I.F., Murty, V.K. and Xu, G. (2008). Non-adjacent Radix-T Expansions of Integers in Euclidean Imaginary Quadratic Number Fields. Canadian Journal of Mathematics 60 (60): 1267-1282.

Hakuta, K., Sato, H. and Takagi, T. (2010). Efficient Arithmetic on Subfield Elliptic Curve over Small Finite Fields of Odd Characteristic Ic. Journal of Mathematical Cryptology 4 (3): 199-238.

Heuberger, C. (2010). Redundant T-adic Expansions II: Non-optimality and Chaotic Behaviour. Mathematic in Computer Science 3(2):141-157.

Heuberger, C.and Krenn, D. Retrieved 03/08/2012. Website, http://arxiv.org/abs/1009.0488.

Heuberger, C.and Krenn, D. Retrieved 05/10/2011. Website, http://arxiv.org/pdf/1110.0966.

Karthikeyan S., Jain S.K., Nayar M.P. and Avanzi, R.M., Heuberger, C. and Prodinger, H. (2011). Redundant T-adic Expansions I: Non-Adjacent Digit Sets and their Applications to Scalar Multiplication. Des. Codes Cryptography 58 (2): 173-202.

Kerry, C.F. and Gallagher, P.D. (2013). Website, http://dx.doi.org/10.6028/NIST.FIPS.186-4.

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.

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.

Mohd Suberi, S., Yunos, F. and Md Said, M.R. (2016). An Even and Odd Situation for the Multiplier of Scalar Multiplication with Pseudo τ-adic Non-Adjacent Form. In Advances in Industrial and Applied Mathematics: Proceedings of 23rd Malaysian National Symposium of Mathematical Sciences (SKSM23). AIP Publishings, Vol 1750. p. 050009.

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., 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. Accepted on 17 December 2012. Publication in JST Vol. 22(2) Jul.2014: 489-506.

Yunos, F., Mohd Atan, K.A., Md Said, M.R. and Kamel Ariffin, M.R. (2015). Pseudo τ-adic Non Adjacent Form for Scalar multiplication on
Koblitz Curves. Malaysian Journal of Mathematical Sciences 9(S)(Special Issue: The 4th International Cryptology and Information Security Conference 2014):71-88·

Yunos, F., Mohd Atan, K.A., Md Said, M.R. and Kamel Ariffin, M.R. (2015). Kembangan Pseudotnaf bagi Pendaraban Skalar ke atas Lengkuk Koblitz. Ph.D. thesis, Universiti Putra Malaysia.

Yunos, F. and Mohd Atan, K.A. (2016). Improvement to Scalar Multiplication on Koblitz curves by using Pseudo τ-adic non-adjacent Form.
In Advances in Industrial and Applied Mathematics: Proceedings of 23rd Malaysian National Symposium of Mathematical Sciences
(SKSM23). AIP Publishing, Vol 1750. p. 050006.

Yunos, F., Mohd Suberi, S., Said Husain, Sh.K., Kamel Ariffin, M.R. and Asbullah, M.A. (2018). On Some Specific Patterns of $\boldsymbol{\tau}$-Adic Non-Adjacent Form Expansion over Ring Z($\boldsymbol{\tau}$). International Journal of Engineering and Applied Sciences. Accepted on Nov 2018.

APPENDIX A

Example A1.

Find pseudoTNAF of $1-4\tau$ as follows.
Consider $\bar{n}=1-4\tau$ and $\bar{\tau}=1-\tau$ is the conjugate of τ. First, $\tau\cdot\bar{\tau}=2$ is shown.

$$\tau\cdot\bar{\tau}=\tau(1-\tau)$$
$$=-\tau^2+\tau$$
$$=-\tau+2+\tau$$
$$=2.$$

Next, the next steps in obtaining pseudoTNAF$(1-4\tau)$ are shown.

Step 1: Since $1-4\tau$ is not divisible by τ, we choose $c_0=1$. Therefore the next coefficient must be 0. That is $c_1=0$.

$$\frac{1-4\tau-1}{\tau}=-4.$$

Therefore, pseudoTNAF$(1-4\tau)=[1,c_1,c_2,\ldots,c_{l-2},c_{l-1}]$.

Step 2: Since -4 is divisible by τ, then $c_1 = 0$.

$$\frac{-4}{\tau} = \frac{-4}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} = \frac{-4 \cdot (1-\tau)}{2} = -2 + 2\tau.$$

Then, pseudoTNAF$(1 - 4\tau) = [1, 0, c_2, \dots, c_{l-2}, c_{l-1}]$.

Step 3: $-2 + 2\tau$ is divisible by τ. Therefore, $c_2 = 0$.

$$\frac{-2+2\tau}{\tau} = \frac{-2}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} + 2 = \frac{-2 \cdot (1-\tau)}{2} + 2 = 1 + \tau$$

Therefore, pseudoTNAF$(1 - 4\tau) = [1,0,0, c_3, c_4, \dots, c_{l-2}, c_{l-1}]$.

Step 4: Since $1 + \tau$ is not divisible by τ then c_3 is -1.

$$\frac{1+\tau+1}{\tau} = \frac{2+\tau}{\tau} = \frac{2}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} + 1 = 2 - \tau.$$

Then, pseudoTNAF$(1 - 4\tau) = [1,0,0, -1, c_4, \dots, c_{l-2}, c_{l-1}]$.

Step 5: $2 - \tau$ is not divisible by τ. Then, we take $c_4 = 0$.

$$\frac{2-\tau}{\tau} = \frac{2}{\tau} - 1 = -\tau.$$

Then, pseudoTNAF$(1 - 4\tau) = [1,0,0, -1,0, c_5, \dots, c_{l-2}, c_{l-1}]$.

Step 6: Since $-\tau$ is divisible by τ then $c_5 = 0$.

$$\frac{-\tau}{\tau} = \frac{-\tau}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} = -1.$$

Then, pseudoTNAF$(1 - 4\tau) = [1,0,0, -1,0,0, c_6, \dots, c_{l-2}, c_{l-1}]$.

Step 7: Since -1 is not divisible by τ then $c_6 = -1$.

$$\frac{-1+1}{\tau} = 0.$$

Lastly, pseudoTNAF$(1 - 4\tau) = [1,0,0, -1,0, 0, -1] = 1 - \tau^3 - \tau^6$. It has 7 digits in size and 4 of Hamming weights.

We used point $P = (x^2, x + 1)$ in the form of polynomial basis which is satisfying E_1. Choose irreducible polynomial $x^3 + x + 1$, then we get the output of scalar multiplication is $Q = (x, x^2 + x + 1)$. The algorithm for scalar multiplication for pseudoTNAF can be refer to Yunos et al. (2016)

Proposition A2. (Yunos et al. , 2018)
Let k be a non-negative integer and TNAF(1)= [1]. The TNAF expansion of $5 + 4k$ is equal to $[1, c_1, c_2, \dots, c_{l-1}]$ where $c_i \in \{-1, 0, 1\}$, $i = 1,2, \dots, l-1$ and l is the length of the expansion.

Proof. By Lemma 1.1, $\alpha = c + d\tau$ where $c = 5 + 4k$ and $d = 0$. Then,

$$\frac{5+4k}{\tau} = \frac{5+4k}{2}t - \frac{5+4k}{2}\tau \notin Z(\tau).$$

We choose $c_0 = 1$, such that $c_i c_{i+1} = 0$. Thus,

$$\frac{5-1+4k}{\tau} = \frac{4+4k}{\tau}$$
$$= \frac{2(2+2n)}{\tau}$$
$$= \frac{2t(2+2k)}{2} - \frac{2(1+k)}{2}\tau$$
$$= 2t(1+k) - (1+k)\tau \in Z(\tau).$$

Thus, the first remainder, c_0 is 1 so that $5 + 4k$ is divisible by τ. Therefore, TNAF expansion of $5 + 4k$ is $[1, c_1, c_2, \dots, c_{l-1}]$ where $c_i \in \{-1, 0, 1\}$ for $i = 1,2, \dots, l-1$.