Journal of Engineering and Applied Sciences 14 (23): 8609-8615, 2019
ISSN: 1816-949X

On Some Specific Patterns of •-Adic Non-Adjacent Form Expansion over Ring Z(•)

[1, 2]F. Yunos, [3]S.M. Suberi, [1, 2]Sh.K. Said Husain, [1, 2]M.R.K Ariffin and [1]M.A. Asbullah
[1]Laboratory of Cryptography, Analysis and Structure,
Institute for Mathematical Research (INSPEM), Serdang, Malaysia
[2]Department of Mathematics, Faculty of Science,
Universiti Putra Malaysia, 43400 Serdang, Malaysia
[3]Infineon Plant, Jalan A7, Kulim High Tech, Kulim, Kedah, Malaysia
faridahy@upm.edu.my, syahirahsuberi@ymail.com, kartini@upm.edu.my, rezal@upm.edu.my,
ma_asyraf@upm.edu.my

Abstract: Let $\tau = (-1)^{1-a} + \sqrt{-7}/2$ for a• {0, 1} is Frobenius map from the set $E_a(F_2\ m)$ to it self for a point (x, y) on Koblitz curves E_a. Let P and Q be two points on this curves. •-adic Non-Adjacent Form (TNAF) of • an element of the ring Z(•) = {• = c+d•|c, d•Z} is an expansion where the digits are generated by successively dividing • by •, allowing remainders of -1, 0 or 1. The implementation of TNAF as the multiplier of scalar multiplication nP = Q is one of the technique in elliptical curve cryptography. In this study, we find the formulas for TNAF that have specific patterns [0, c_1, ..., c_{1-1}], [-1, c_1, ..., c_{1-1}], [1, c_1, ... c_{1-1}] and [0, 0, 0, c_3, c_4, ..., c_{1-1}].

Key words: Koblitz curve, •-adic non-adjacent form, Frobenius map, successively, TNAF, expansion, element

INTRODUCTION

The Koblitz curves are a special type of curves for which the Frobenius endomorphism can be used for improving the performance of computing an elliptic scalar multiplication (Koblitz, 1987). It is defined over F_2m 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, 1992). The Frobenius map $\tau = (-1)^{1-a} + \sqrt{-7}/2$ from the set $E_a\ (F_2^m)$ to itself for a point (x, y) on E_a. Scalar multiplication involves computing integer for multiple times for an integer n and P, nP = Q where, P and Q are points on Koblitz curve. Figure 1 by Yunos and Atan (2016) gives an illustration of the scalar multiplication in this set but in this study, we are implementing the secret key n = • in the form of TNAF (refer definition 2.1).

TNAF was first developed by Solinas, 1997. The digits of TNAF of • are generated by successively dividing • with •, allowing the remainders to-1, 0 or 1. The following lemma is due to Solinas (2000) which explains division of an element in Z(•).

Lemma1.1: Let • = c+d••Z(•). Then:

- • is divisible by •, if and only if c is even. That is, •/• = (d+tc/2)-c/2 where, $t = (-1)^{1-a}$ for. a• {0, 1}. If c is odd, then the remainder is chosen either 1 or -1
- • is divisible by $\bullet^2$ if and only, if c • 2d (mod 4)

TNAF representation of • can be written as TNAF (•) = [c_0, c_1, c_2, ..., c_{1-2}, c_{1-1}]. The coefficients, c_i of TNAF are generated repeatedly by dividing • with • until, c and d are equal to 0. If is not divisible by •, we choose remainder either 1 or -1. The next coefficient (c_i+1) of TNAF expansion after must be 0, since, c_ic_{i+1} = 0. The division process, for example, TNAF (8) is in appendix A. Based on lemma 1.1 (Solinas, 2000) developed algorithm 1 for finding TNAF (c+d•). This is one of the most efficient algorithms of scalar multiplication on Koblitz curve because it can eliminate the elliptic doublings in the scalar multiplication and double the number of elliptic additions. It can help us to list all the patterns of TNAF(c) in Table 1.

Algorithm 1; TNAF expansion:

```
Input: integers c, d
Output: TNAF (c+d•)
Computation:
        1. Set c0• c, c1• d
        2. Set S• <>
```

Corresponding Author: F. Yunos, Laboratory of Cryptography, Analysis and Structure,
Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, 43400 Serdang, Malaysia,
faridahy@upm.edu.my

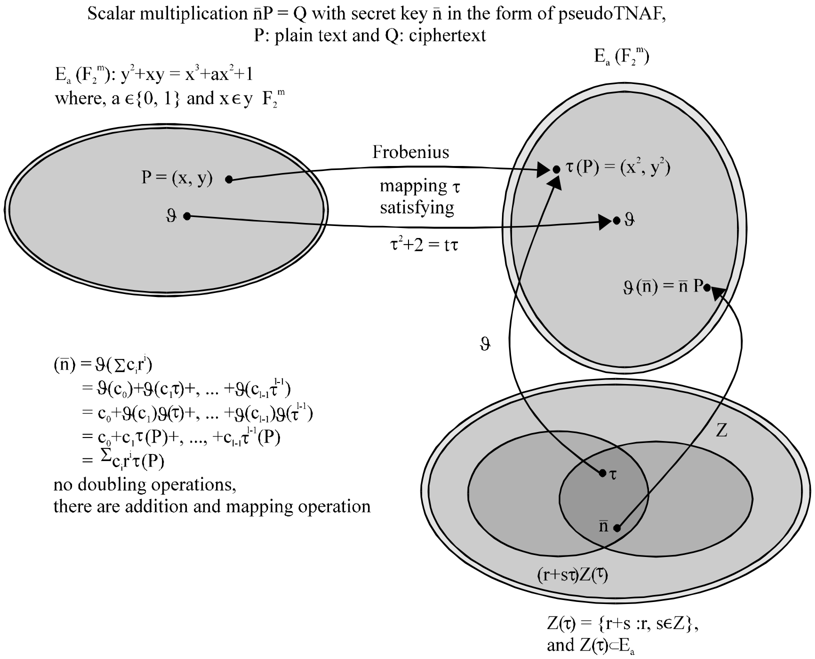
Scalar multiplication n̄P = Q with secret key n̄ in the form of pseudoTNAF,
P: plain text and Q: ciphertext
$E_a (F_2^m)$: $y^2+xy = x^3+ax^2+1$
where, a ϵ{0, 1} and x ϵ y F_2^m
$E_a (F_2^m)$
P = (x, y)
ϑ
Frobenius
mapping τ
satisfying
$\tau^2+2 = t\tau$
$\tau(P) = (x^2, y^2)$
ϑ
ϑ(n̄) = n̄ P
ϑ
Z
τ
n̄
(r+sτ)Z(τ)
$Z(\tau) = \{r+s :r, s\epsilon Z\}$,
and $Z(\tau) \subset E_a$
$(\bar{n}) = \vartheta(\Sigma c_i r^i)$
$= \vartheta(c_0)+\vartheta(c_1\tau)+, ... +\vartheta(c_{l-1}\tau^{l-1})$
$= c_0+\vartheta(c_1)\vartheta(\tau)+, ... +\vartheta(c_{l-1})\vartheta(\tau^{l-1})$
$= c_0+c_1\tau(P)+, ..., +c_{l-1}\tau^{l-1}(P)$
$= \Sigma c_i r^i \tau(P)$
no doubling operations,
there are addition and mapping operation

Fig. 1: An illustration of scalar multiplication in the set F_2^m

Table 1: The TNAF expansion of integer from 1-21 and its HW and length (l)

c	TNAF(c)	HW	Length (l)
1	[1]	1	1
2	[0,-1,0,-1]	2	5
3	[-1,0,1,0,0,-1]	3	6
4	[0,0,1,0,0,1]	2	6
5	[1,0,1,0,0,1]	3	6
6	[0,1,0,0,0,1]	2	6
7	[-1,0,0,-1,0,1]	3	6
8	[0,0,0,-1,0,1]	2	6
9	[1,0,0,-1,0,0,1]	3	6
10	[0,-1,0,0,-1,0,-1,0,-1]	4	9
11	[-1,0,-1,0,-1,0,-1,0,-1]	5	9
12	[0,0,-1,0,-1,0,-1,0,-1]	4	9
13	[1,0,-1,0,-1,0,-1,0,-1]	5	9
14	[0,1,0,-1,0,0,-1,0,-1]	4	9
15	[-1,0,0,0,1,0,0,0,-1]	3	9
16	[0,0,0,0,1,0,0,0,-1]	2	9
17	[1,0,0,0,1,0,0,0,-1]	3	9
18	[0,-1,0,1,0,1,0,0,-1]	4	9
19	[-1,0,1,0,-1,0,0,1,0,0,1]	5	11
20	[0,0,1,0,-1,0,0,1,0,0,1]	4	11
21	[1,0,1,0,-1,0,0,1,0,0,1]	5	11

```
3. While $c_0$ •  0 or $c_1$ •  0
4.  If $c_0$ odd then
5.        set u• 2-($c_0$-2$c_1$ mod 4)
6.        set $c_0$• $c_0$-u
7.  else
8.        set u• 0
9.  Prepend u to S
10.       Set ($c_0$, $c_1$)• ($c_1$+t$c_0$/2-$c_0$/2)
11. End While
12. Output
```

Moreover, Solinas (1997, 2000) gave the main properties of TNAF as follows:

Theorem 1.3: Let • •Z(•) and • • 0 then TNAF(•) is a unique digit representation. If the length l(•) is greater than, 30 then:

$$\log_2 N(\alpha)-0.55 < l(\alpha) < \log_2 N(\alpha)+3.52$$

where, N(•) is the norm of • . The average density of non-zero digits in the expansion of l is approximately 1/3. Other properties of TNAF also have been studied and developed by some researchers such as Avanzi *et al.* (2006, 2011), Hakuta *et al.* (2010), Koblitz (1987), Blake *et al.* (2008), Heuberger (2010), Avanzi *et al.* (2011), Heuberger and Krenn (2013) for scalar multiplication on Koblitz curve and some type of the other curves.

Recently, PseudoTNAF of • modulo • •^{m}-1/•-1 for scalar multiplication on Koblitz curve was developed by Yunos *et al.* (2014), Yunos *et al.* (2015a, b), Yunos and Atan (2016), Yunos *et al.* (2018), Blake *et al.* (2008) and Suberi and Yunos (2018c). Besides that, they introduced the following theorem which helps in the transformation of pseudoTNAF expansion into an element Z(•) by implementing Lucas sequence (Definition 2.4).

Theorem 1.4: If $a_0 = 0$, $b_0 = 1$, $a_i = a_{i-1}+b_{i-1}$ and $b_i = -2a_{i-1}$ for i>0, then:

$$\tau^i = b_i t^i + a_i t^{i+1}\tau$$

This theorem can help in the conversion of TNAF into an element of Z(•) as in the following theorem.

Table 2: TNAF with $c_0, c_{l-1} = \pm 1$ and $c_1 = c_2 = , \bullet , = c_{1-2} = 0$ with its r+s• for 3• l• 15

TNAF expansion	r+s•	Length (l)
±[1,0,1]	±(-1+•)	3
±[1,0,0,1]	±(-1-•)	4
±[1,0,0,1]	±(3-3•)	5
±[1,0,0,0,1]	±(7-•)	6
±[1,0,0,0,0,1]	±(3+5•)	7
±[1,0,0,0,0,0,1]	±(-9+7•)	8
±[1,0,0,0,0,0,0,1]	±(-13-3•)	9
±[1,0,0,0,0,0,0,0,1]	±(-7-17•)	10
±[1,0,0,0,0,0,0,0,0,1]	±(35-11•)	11
±[1,0,0,0,0,0,0,0,0,0,1]	±(23+23•)	12
±[1,0,0,0,0,0,0,0,0,0,0,1]	±(-45+45•)	13
±[1,0,0,0,0,0,0,0,0,0,0,0,1]	±(-89-•)	14
±[1,0,0,0,0,0,0,0,0,0,0,0,0,1]	±(-3-91•)	15

Table 3: TNAF with $c_0 = \bullet 1$, $c_{l-1} = \pm 1$ and $c_1 = c_2 = , \bullet , = c_{1-2} = 0$ with its r+s• for 3• l• 15

TNAF expansion	r+s•	Length (l)
±[-1, 0, 1]	±(-3+•)	3
±[-1, 0, 0, 1]	±(-3-•)	4
±[-1, 0, 0, 1]	±(1-3•)	5
±[-1, 0, 0, 0, 1]	±(5-•)	6
±[-1, 0, 0, 0, 0, 1]	±(1+5•)	7
±[-1, 0, 0, 0, 0, 0, 1]	±(-11+7•)	8
±[-1, 0, 0, 0, 0, 0, 0, 1]	±(-15-3•)	9
±[-1, 0, 0, 0, 0, 0, 0, 0, 1]	±(5-17•)	10
±[-1, 0, 0, 0, 0, 0, 0, 0, 0, 1]	±(33-11•)	11
±[-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]	±(21+23•)	12
±[-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]	±(-47+45•)	13
±[-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]	±(-91-•)	14
±[-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]	±(181-89•)	15

Theorem 1.5: If $a_0 = 0$, $b_0 = 1$, $a_i = a_{i-1}+b_{i-1}$ and $b_i = -2a_{i-1}$, then:

$$\sum_{i=0}^{l-1} c_i \tau^i = r+s\tau$$

Where:

$$r = \sum_{i=0}^{l-1} c_i\ b_i\ t^i$$

$$s = \sum_{i=0}^{l-1} c_i\ a_i\ t^{i+1} \text{ for i, l>0}$$

Based on theorems 1.4 and 1.5 (Solinas, 1997) developed the following algorithm for converting $\mathrm{TNAF}\left(\sum_{i=0}^{l-1} c_i \tau^i\right)$ to an element of Z(•) and its programming in Maple 15. It helps them in listing all the TNAF's with patterns $[c_0, 0, ..., 0, c_{l-1}]$ and $[c_0, 0, 0, ..., c_{l-1}/2, ..., 0, c_{l-1}]$ for $c_0, 0, 0, ..., c_{l-1}/2\ c_{l-1} \bullet \{-1, 1\}$, In this research, we can consider r+s• = c+d•.

Algorithm 2; (Converting to $\bullet_{i=0}^{l-1} c_i \bullet^{1}$ to r+s••z(•)):

Input: Coefficient of TNAF($[c_0, c_1, ..., c_{l-2}, c_{l-1}]$), trace $t = (-1)^{1-a}$ for a = 0 or a = 1

Output: r+s••Z(•)

Computation:

```
1. $a_0 \bullet 0$, $b_0 \bullet 1$
2. for i from l-1 do
3.       $a_i \bullet a_{i-1}+b_{i-1}$
4.       $b_i \bullet -2a_{i-1}$
5.       $g_{i-1} \bullet a_{i-1}t_i$
6.       $h_{i-1} \bullet b_{i-1}t^{i+1}$
7. end do
8.       $r \bullet \bullet_{i=1}^{l} c_i h_i$
9.       $S \bullet \bullet_{i=1}^{l} c_i g_{i-1}$
10. return to (r, s)
```

Table 4: TNAF with c_0, $c_{l-1}/2$, $c_{l-1} = \bullet 1$ and $c_1 = c_2 = , \bullet , = c_{1-2} = 0$ with its r+s• for l = 5,7,9, • , 21

TNAF expansion	r+s•	Length (l)
±[1,0,1,0,1]	±(1-2•)	5
±[1,0,0,1,0,0,1]	±(1+4•)	7
±[1,0,0,0,1,0,0,0,1]	±(-11-6•)	9
±[1,0,0,0,0,1,0,0,0,0,1]	±(41-12•)	11
±[1,0,0,0,0,0,1,0,0,0,0,0,1]	±(-43+50•)	13
±[1,0,0,0,0,0,0,1,0,0,0,0,0,0,1]	±(-7-84•)	15
±[1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1]	±(165+90•)	17
±[1,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1]	±(-535+68•)	19
±[1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,1]	±(949-636•)	21

As a result, they developed propositions 1.7 and 1.8 by Solinas (1997) for describing the TNAF's with patterns (refer to Table 2 and 3) and $[c_0, 0, ..., c_{l-1}/2, ..., c_{l-1}$ (refer to Table 4), respectively.

Proposition 1.7: Let l• 3, $a_0 = 0$ and $b_0 = 1$. If $\bullet^i = b_i t^i + a_i t^{i+1} \bullet$ for $a_i = a_{i-1}+b_{i-1}$ and $b_i = -2a_{i-1}$, then:

$$c_0 + c_{l-1}\ \tau^{l-1} = \left(c_0 + c_{l-1}\ b_{l-1}\ t^{l-1}\right) + \left(c_{l-1} a_{l-1} t^{l}\right)\tau$$
$$\text{for } t, c_0, c_{l-1} \in \{-1, 1\}$$

Proposition 1.8: Let, l = 3+ 2• for • be a natural number, a_0, = 0, $b_0 = 1$ and t•{-1, 1}. If $\bullet^i = b_i t^{i+1} \bullet$ for $a_{i-1}+b_{i-1}$ and $b_i = -2_{i-1}$ then:

$$\pm\left(1 + \tau^{\frac{l-1}{2}} + \tau^{l-1}\right) = \left(\left(1 + b_{\frac{l-1}{2}} t^{\frac{l-1}{2}} + b_{l-1} t^{l-1}\right) + \left(a_{\frac{1-1}{2}} t^{\frac{l-1}{2}+1} a_{l-1} t^{l}\right)\tau\right)$$

Hence, we already know the two patterns of TNAF's as mentioned above. Meaning that, we should avoid to choose the secret key n (such that nP = Q) with such expansion for cryptographic purposes. To achieve the similar objective, we examine another four patterns of TNAF expansion in the form of $[0, c_1, ..., c_{l-1}]$ $[-1, c_1, ..., c_{l-1}]$ $[1, c_1, ..., c_{l-1}]$ and $[0, 0, 0, c_3, c_4, ..., c_{l-1}]$. It can help the third party to trace the first, second and third coefficients of n.

MATERIALS AND METHODS

Preliminaries: The following are some definitions can be found by Hankerson *et al.* (2006), Yunos (2015a), Yunos *et al.* (2014, 2015b, c), Hafizah and Yunos (2018a), Yunos and Suberi (2018b, c), Suberi *et al.* (2016a), Yunos and Atan (2016) and Solina (2000) that will be used throughout this study.

Definition 2.1: •-adic non-adjacent form (also called •- NAF or TNAF) of nanozero • in Z(•) is equal to $\bullet_{i=0}^{l-1} c_i \bullet^i$ where, $c_i \bullet \{-1, 0, 1)$ and $c_i c_{l+1} = 0$ for all i. If $c_{l-1} \bullet 0$ then l is said to be the length of TNAF.

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

Definition 2.2: The norm of, • = c+d• is the integer product of • and its complex conjugate $\bar{\alpha}$ Explicitly, N(•) = c^2+tcd+2d^2 where, t = $(-1)^{1-a}$ and • • {0, 1}.

Definition 2.3: A Hamming Weight (HW) is defined as the number of coefficients 1 and -1 in the expansion of an element of Z(•).

Definition 2.4: Given two integer parameters P and Q, the Lucas sequences of the first kind U_n(P, Q) and of the second kind V_n(P, Q) are defined by the recurrence relations:

$$U_0(P, Q) = 0, U_1(P, Q) = 1 \text{ and } U_n(P, Q) = PU_{n-1}(P, Q)\text{-}QU_{n-2}(P, Q)$$

And:

$$V_0(P, Q) = 2, V_1(P, Q) = P \text{ and } V_n(P, Q) = PV_{n-1}(P, Q)\text{-}QV_{n-2}(P, Q)$$

for n>1. In our case, we refer to the Lucas sequence of the first kind defined and U_0 = 0, U_1 = 1 and U_i = tU_{i-1}-2U_{i-2} for i• 2 where, t = $(-1)^{1-a}$ for a• {0, 1}.

Definition 2.5: An average of Hamming weight among TNAF expansion for an element in Z(•) that have length l is defined as the Hamming weight among TNAF divided by the number of combination of c_i and t where, c_i is the coefficient of TNAF expansion and t is the trace of Frobenius endomorphism.

Definition 2.6: An average density among TNAF for an element of Z(•) having length l is defined by the average Hamming weight among TNAF divided by the length l.

RESULTS AND DISCUSSION

The coefficients c_i can have the values -1, 0, 1. We identify cases for integers that have different value for c_0. We begin first by observing the TNAF expansions of integers varying from 1-21. The TNAF expansion for each c+d• is attained based on lemma 1.1. By referring to this lemma, we have c+d• = c+0• in element of Z(•). Let TNAF (c) = [c_0, c_1, ..., c_{l-1}] where l is the length of the expansion and c_i for i = 0, 1, 2, ..., l-1 are the coefficients of TNAF expansion. The coefficients, c_i of TNAF (c) are generated by dividing c with •, allowing the value of c_i can be either 0 or±1. The steps are repeated until the quotient of each division with • equals to 0. Table 1 shows TNAF expansion of integer c starting from integer c = 1 up to c = 21, respectively with its HW and length of the expansion. In Table 1, we consider four patterns of TNAF expansions in the form of [0, c_1, ..., c_{l-1}] [-1, c_1, ..., c_{l-1}] [1, c_1, ..., c_{l-1}] and [0, 0, 0, c_3, c_4, ..., c_{l-1}].

Based on Table 1, we have three categories of c_0, the first coefficient of each TNAF expansion. The first case is when c_0 = 0. The sequences having the first coefficient equal to 0 are as follows: [0, -1, 0, -1] [0, 0, 1, 0, 0, 1] [0, 1, 0, 0, 0, 1] [0, 0, 0, -1, 0, 1] [0, -1, 0, 0, -1, 0, -1, 0, -1] [0, 0, -1, 0, -1, 0, 1, 0, -1] [0, 1, 0, -1, 0, 0, -1, 0, -1] [0, 0, 0, 0, 1, 0, 0, 0, -1] [0, -1, 0, 1, 0, 1, 0, 0, -1] and [0, 0, 1, 0, -1, 0, 0, 1] for c = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20. Proposition 3.1 explains the TNAF expansion of the first case.

Proposition 3.1: Let k be a non-negative integer. The TNAF expansion of 2+2k is equal to [0, c_1, ..., c_{l-1}] where, c_i• {-1, 0, 1}, i = 1, 2, ..., l-1 and l is the length of the expansion.

Proof: From lemma 1.1, since, 2+2k is even, then, 2+2k is divisible by •. That is:

$$\frac{2+2k}{\tau} = t(t+tk)\text{-}(1+k)\tau \in Z(\tau)$$

It implies that the first coefficient, c_0 is 0. Then, TNAF expansion of 2+2k is [0, c_1, ..., c_{l-1}]. The following example is an illustration of proposition 3.1.

Example 1: By referring Table 1, we choose TNAF(20). Since, 20 is in the form 2+2(9), it is proven that by proposition 3.1, the first coefficient is 0.

The next proposition shows that second case in which the first coefficient of TNAF expansion c_0 = -1. From Table 1, the sequences having the first coefficient equal to -1 are as follows: [-1, 0, 1, 0, 0, -1] [-1, 0, 0, -1, 0, 1] [-1, 0, -1, 0, -1, 0, -1 0, -1] [-1, 0, 0, 0, 1, 0, 0, 0, -1] and [-1, 0, 1, 0, -1, 0, 0, 1, 0, 0, 1] for c = 3, 7, 11, 15 and 19.

Proposition 3.2: Let k be a non-negative integer. The TNAF expansion of 3+4k is equal to [-1, c_1, ..., c_{l-2}, c_{l-1}] where c_i• {-1, 0, 1}, i = 1, 2, ..., l-1 and l is the length of the expansion.

Proof: From lemma 1.1, • = c+d• where c = 3+4k and d = 0. Then:

$$\frac{3+4k}{\tau} = \frac{3+4k}{2}\text{-}\frac{3+4k}{2}\tau \notin Z(\tau)$$

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

$$\begin{aligned}\frac{3\text{-}(\text{-}1)+4k}{\tau} &= \frac{4+4k}{\tau}\\ &= \frac{2(2+2k)}{\tau}\\ &= \frac{2t(2+2k)}{2}-\frac{2(1+k)}{2}\tau\\ &= 2t(1+k)-(1+k)\tau\in Z(\tau)\end{aligned}$$

Thus, the first remainder c_0 is so that, 3+4k is divisible by •. The TNAF expansion of is 3+4k is [-1, c_1, ... $c_{l\text{-}3}$, $c_{l\text{-}2}$, $c_{l\text{-}1}$]. Example 2 describes proposition 3.2.

Example 2: By referring Table 1, we choose TNAF(19). The value 19 is in the form of 3+4(4), then, it is proven that by proposition 3.2, c_0 = -1. The second coefficient of 19 must be 0, so that, c_ic_{i+1} = 0.

The next proposition explains the third case in which the first coefficient c_0 = 1. From Table 1, the sequences having the last coefficient equal to 1 are as follows: [1], [1, 0, 1, 0, 0, 1] [1, 0, 0 -1, 0, 1] [1, 0, -1, 0, -1, 0, -1, 0, -1, 0, -1] [1, 0, 0, 0, 1, 0, 0, 0, -1] and [1, 0, 1, 0, -1, 0, 0, 1, 0, 0, 1] for c = 1, 5, 9, 13, 17 and 21.

Proposition 3.3: 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, ..., $c_{l\text{-}1}$] where, c_i• {-1, 0, 1} i = 1, 2, ..., l-1 and l is the length of the expansion.

Proof: By lemma 1.1 a = c+d• where c = 5+4k and d = 0. Then:

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

We choose c_0 = 1 such that c_ic_{i+1} = 0. Thus:

$$\begin{aligned}\frac{5\text{-}1+4k}{\tau} &= \frac{4+4k}{\tau}\\ &= \frac{2(2+2k)}{\tau}\\ &= \frac{2t(2+2k)}{2}-\frac{2(1+k)}{2}\tau\\ &= 2t(1+k)-(1+k)\tau\in Z(\tau)\end{aligned}$$

Thus, the first remainder c_0 is 1, so that, 5+4k is divisible by •. Therefore, TNAF expansion of 5+4k is [1, c_1, c_2, ..., $c_{l\text{-}1}$] where, c_i• {-1, 0, 1} for i = 1, 2, ..., l-1. We give the following example to explain proposition 3.3.

Example 3: By referring Table 1, we choose TNAF (21). Since, 21 is in the form of, it is proven that by proposition 3.3, then the first coefficient is 1. The second coefficient is 0, c1 = 0 for the expansion satisfying c_i• {-1, 0, 1}.

Table 1 shows Hamming weight of TNAF(3+4k) is equal to Hamming weight of TNAF(5+4k) for non-negative integer, k. For example, HW TNAF(7) = HW TNAF(9), HW TNAF (11) = HW TNAF(13) and HW TNAF(15) = HW TNAF(17). Obviously, HW for TNAF (2+2k) is less one than the HW for TNAF(3+4k) or TNAF (5+4k). Now, from Table 1 we deliver the last case in which the first, second and third coefficients of TNAF expansion are 0, 0 and 0, respectively. The sequences are as follow: [0, 0, 0, -1, 0, 1] and [0, 0, 0, 0, 1, 0, 0, 0, -1] for c = 1,5. Proposition 3.4 describes this patterns.

Proposition 3.4: Let k_1 and k_2 be a natural number, then:

$$\text{TNAF}(8k_1+8k_2\tau)=[0,0,0,c_3,c_4,...,c_{l\text{-}1}]$$

where, c_0, c_1, c_2 = 0 such that c_i• {-1, 0, 1} for i = 3, 4, ..., l-1 and l is the length of the expansion.

Proof: Suppose • = c+d• where c = $8k_1$ and d = $8k_2$.We proceed with finding TNAF ($8k_1+8k_2$•).

Step 1: Since, • = $8k_1+8k_2$• is divisible by •, then c_0 = 0:

$$\frac{\alpha}{\tau}=\frac{8k_1+8k_2\tau}{\tau}= \\ 4k_1t+8k2\text{-}4k_1\tau\in Z(\tau)$$

Thus, TNAF($8k_1+8k_2$•) = [0, c_1, c_2, ..., $c_{l\text{-}1}$].

Step 2: Since, $4k_1t+8k_2\text{-}4k_1$• is divisible by •, then c_1 = 0:

$$\frac{4k_1t+8k_2\text{-}4k_1\tau}{\tau}=4k_1t+4k_2t+2k_1t^2\text{-}(2k_2k_1+4k_2)\tau\in Z(\tau)$$

Thus, TNAF($8k_1+8k_2$•) = [0, 0, c_1, c_2, ..., $c_{l\text{-}1}$].

Step 3: Since, $\text{-}4k_1t+4k_2t+2k_1t^2\text{-}(2k_2k_1+4k)$• is divisible by •, then c_2 = 0:

$$\frac{\text{-}4k_1t+4k_2t+2k_1t^2\text{-}(2k_2k_1+4k)\tau}{2}= \\ -4k_2\text{-}2k_1k_2\text{-}2k_1t^2+2k_2t^2+2k_1t^3+ \\ (2k_1\text{-}2k_2t\text{-}k_1t^2)\tau\in Z(\tau)$$

Then, TNAF($8k_1+8k_2$•) = [0, 0, 0, c_3, ..., $c_{l\text{-}1}$]. The value $8k_1+8k_2$• is divisible by • for t = -1 or t = 1. Therefore, the first coefficient, c_0 is 0. For the second division, $4k_1t+8k_2\text{-}4k_1$• is divisible by •, therefore, the remainder, c_1 is 0. Element -4jt+4kt+2jt^2-(2kj+4k)• is also divisible by •, hence, the third remainder c_2 is 0. Therefore, TNAF expansion of $8k_1+8k_2$• is [0, 0, 0, c_3, ..., $c_{l\text{-}2}$, $c_{l\text{-}1}$]. The following is the example of proposition 3.4.

Example 4: By referring Table 1, we choose TNAF(8) = [0, 0, 0, ..., 1, 0, 1] Since, 8 is in the form of 8(1)+8(0)• by proposition 3.4, then the first three coefficients are 0.

CONCLUSION

From propositions 3.1-3.4, we conclude that the expected patterns of TNAF with certain form of integers c are as follow:

Integer c	Expected patterns of TNAF (c)
2+2k for k• W	$[0, c_1, ..., c_{l-1}]$
3+4k for k• W	$[-1, c_1, ..., c_{l-1}]$
5+4k for k• W	$[1, c_1, ..., c_{l-1}]$
$8k_1+8k_2$ • for k_1, k_2• N	$[0, 0, 0, c_3, c_4, ..., c_{l-1}]$

It can help the attackers to trace the first, second and third coefficients of the secret key n (such that nP = Q) where, n is in the form of TNAF's expansion.

ACKNOWLEDGEMENT

The researchers are grateful to Universiti Putra Malaysia for a support via. Geran Putra GP/2018/9595400 and MyBrain15.

APPENDIX A

Example 5: Consider • = 8+0• c = 8, d = 0, a = 1 and $\bar{\tau}$ = 1- • is the conjugate of •. First, $\tau\bar{\tau}$ = 2 is shown:

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

Next, the steps in obtaining TNAF (8) are shown.

Step 1: Since, 8 is divisible by, •, we choose c_0 = 0. The remainder is 0. Therefore, the next coefficient may be 0, -1 or 1. That is c_1• {-1, 0, 0}:

$$\frac{8}{\tau} = \frac{8}{\tau}.\frac{\bar{\tau}}{\bar{\tau}}\frac{8(1-\bar{\tau})}{2} = 4-4\tau$$

Therefore, TNAF(8) = $[0, c_1, c_2, ..., c_{l-2}, c_{l-1}]$.

Step 2: Since, 4-4• is divisible by •, then, c_1 = 0:

$$\frac{4-4\tau}{\tau} = \frac{4}{\tau}-4 = \frac{4}{\tau}.\frac{\bar{\tau}}{\bar{\tau}}-4 = -2-2\tau$$

Then, TNAF(8) = $[0, c_1, c_2, ..., c_{l-2}, c_{l-1}]$. Step 3: -2-2• is divisible by •. Therefore, c_2 will be 0:

$$\frac{-2-2\tau}{\tau} = \frac{-2}{\tau}.\frac{\bar{\tau}}{\bar{\tau}}-2 = -3+\tau$$

Therefore, TNAF(8) = $[0, 0, 0, c_3, c_4, ..., c_{l-2}, c_{l-1}]$.

Step 4: Since, -3+• is not divisible by 0, we choose c_3 = -1. The remainder can be either 1 or -1. Therefor, the next coefficient must be 0. That is c_4 = 0:

$$\frac{-3+\tau-(-1)}{\tau} = \frac{-2}{\tau}.\frac{\bar{\tau}}{\bar{\tau}}+1 = \tau$$

Then, TNAF(8) = $[0, 0, 0, -1\ c_4, ..., c_{l-2}, c_{l-1}]$. Step 5. • is divisible by •. Then, c_4 = 0:

$$\frac{\tau}{\tau} = 1$$

Therefore, TNAF(8) = $[0, 0, 0, -1, 0, c_5, ..., c_{l-2}, c_{l-1}]$.

Step 6: Since, 1 is divisible by • then c_5 = 1:

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

Therefore, TNAF(8) = [0, 0, 0, -1, 0, 1].

REFERENCES

Avanzi, R., C. Heuberger and H. Prodinger, 2011. Redundant t-adic expansions I: Non-adjacent digit sets and their applications to scalar multiplication. Des. Codes Cryptography, 58: 173-202.

Avanzi, R.M., C. Heuberger and H. Prodinger, 2006. On redundant t-adic expansions and non-adjacent digit sets. Proceedings of the 13th International Workshop on Selected Areas in Cryptography, August 17-18, 2006, Springer, Berlin, Germany, ISBN: 978-3-540-74461-0, pp: 285-301.

Blake, I.F., V.K. Murty and G. Xu, 2008. Nonadjacent radix-t expansions of integers in Euclidean imaginary quadratic number fields. Canad. J. Math., 60: 1267-1282.

Hadani, N.H. and F. Yunos, 2018. Alternative formula of Tm in scalar multiplication on Koblitz curve. AIP. Conf. Proc., Vol. 1974, 10.1063/1.5041533.

Hakuta, K., H. Sato and T. Takagi, 2010. Explicit lower bound for the length of minimal weight t-adic expansions on Koblitz curves. J. Math. Ind., 2: 75-83.

Hankerson, D., Menezes, A.J. and S. Vanstone, 2006. Guide to Elliptic Curve Cryptography. Springer, Berlin, Germany, ISBN:9780387218465, Pages: 312.

Heuberger, C. and D. Krenn, 2013. Existence and optimality of w-non-adjacent forms with an algebraic integer base. Acta Math. Hungarica, 140: 90-104.

Heuberger, C., 2010. Redundant t-adic expansions II: Non-optimality and chaotic behaviour. Math. Comput. Sci., 3: 141-157.

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209.

Koblitz, N., 1992. CM-curves with good cryptographic properties. Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, Aug. 11-15, Springer Verlag, London, pp: 279-287.

Solinas, J.A., 1997. An improved algorithm for arithmetic on a family of elliptic curves. Proceedings of the International Annual Conference on Cryptology, August 17-21, 1997, Springer, Berlin, Germany, ISBN:978-3-540-63384-6, pp: 357-371.

Solinas, J.A., 2000. Efficient Arithmetic on Koblitz Curves. In: Design, Codes and Cryptography, Solinas, J.A. (Ed.). Springer, Boston, Massachusetts, pp: 195-249.

Suberi, S., F. Yunos, S. Suberi, M.R.S. Said and S.H. Sapar *et al.*, 2018. Formula of t-adic non adjacent form with the least number of NON zero coefficients. J. Karya Asli Lorekan Ahli Math., 11: 23-30.

Suberi, S.M., F. Yunos and M.R.M. Said, 2016. An even and odd situation for the multiplier of scalar multiplication with pseudo t-adic non-adjacent form. AIP. Conf. Proc., 1750: 1-9.

Yunos, F. and K.A.M. Atan, 2016. Improvement to scalar multiplication on Koblitz curves by using pseudo T-adic non-adjacent form. AIP. Conf. Proc., 1750: 1-8.

Yunos, F. and S.M. Suberi, 2018. Even and odd nature for pseudo T-adic non-adjacent form. Malaysian J. Sci., 37: 94-102.

Yunos, F., 2015. Development of pseudo TNAF for aging calculate calling the curlcobitz. Ph.D Thesis, Universiti Putra Malaysia, Seri Kembangan, Malaysia.

Yunos, F., K.A.M. Atan, M.R.K. Ariffin and M.R.M. Said, 2015a. Pseudo-ADIC non adjacent form for scalar multiplication on Koblitz curves. Proceedings of the 4th International Conference on Cryptology and Information Security (Cryptology 2014), June 24-26, 2014, Institute for Mathematical Research, Serdang, Malaysia, pp: 120-130.

Yunos, F., K.A.M. Atan, M.R.K. Ariffin and M.R.M. Said, 2015b. Pseudo-ADIC non adjacent form for scalar multiplication on Koblitz curves. Malaysian J. Math. Sci., 9: 71-88.

Yunos, F., K.A.M. Atan, M.R.M. Said and M.R.K. Ariffin, 2014. A Reduced T-Adic NAF (RTNAF) representation for an efficient scalar multiplication on Anomalous Binary Curves (ABC). Pertanika J. Sci. Technol., 22: 489-505.