Indian Journal of Science and Technology, Vol 9(28), DOI: 10.17485/ijst/2016/v9i28/97358, July 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Maximum and Minimum Norms for τ-NAF Expansion on Koblitz Curve

Nur Adawiah Ali[1]* and Faridah Yunos[2]

[1]Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia; adawiah_nur@ymail.com
[2]Mathematical Department, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia; faridahbintiyunos@gmail.com

Abstract

Background/Objectives: The scalar multiplication in Elliptic Curve Cryptosystem (ECC) is the dominant operation of computing integer multiple for an integer *n* and a point *P* on elliptic curve. In 1997, Solinas[4] introduced the τ-adic non-adjacent form (τ-NAF) expansion of an element *n* of ring Z(τ) on Koblitz Curve. However in 2000, Solinas estimated the length of τ-NAF expansion by using maximum and minimum norms that obtained by direct evaluation method. In 2014, Yunos et al.[9] introduced the formula of norm for every τ-NAF to improve this method. However, a lot of combination of norm should be considered when length of expansion is more than 15. So, the objective of this paper is to built the formulas to calculate the number of maximum and minimum norms for τ-NAF occurring among of all elements in Z(τ). Application/Improvement: With these formulas, we can estimate the length of τ-NAF expansion more accurately.

Keywords: τ-adic Non-Adjacent Form (τ-NAF), Koblitz Curve, Maximum and Minimum Norms

1. Introduction

ECC was proposed by Miller[1] and Koblitz[2]. Koblitz[2] found that the Koblitz curves are a special type of curves for which the Forbenius endomorphism can be used to improve the performance of computing a scalar multiplication. Scalar multiplication of elliptic curve is the operation of successively adding a point along an elliptic curve defined as *nP* where *P* is the point on the curve and *n* is an integer called scalar. Koblitz curve defined over F_{2^m} as follows.

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

with $a \in \{0,1\}$ as suggested by Koblitz[3].The Frobenius map $\tau : E_a\left(F_{2^m}\right) \mapsto E_a(F_{2^m})$ for a point $P = (x, y)$ on $E_a(F_{2^m})$ is defined by

$$\tau(x,y) = \left(x^2, y^2\right), \tau(0) = 0$$

where 0 is the point at ∞. It stands that $(\tau^2 + 2)P = t\tau(P)$ for all $P \in E_a(F_{2^m})$, where the trace $t = (-1)^{1-a}$. The Forbenius map is considered as a multiplication with complex number $\tau = \frac{t + \sqrt{-7}}{2}$.

Other than that, there are several other research have been carried out with the same aim which is to improve or upgrade the performances of scalar multiplication on ECC. Solinas[4] introduced Non-Adjacent Form (NAF) expansion followed by Solinas[5] proposed τ-adic Non-Adjacent Form (τ-NAF) expansion for an integer $n \in Z(\tau)$ to compute scalar multiplication on Koblitz curve more efficiently than the previous version. Solinas[5] also claimed that reduced τ-NAF can be used to replace τ-NAF for scalar multiplication on Koblitz curve since these two expansions are equivalent to each other. Joye and Tymen[6] proposed the randomization of multiplier k by reducing it modulo $\rho(\tau^m - 1)$ from $\tau^m - 1$ to

*Author for correspondence

protect the application of Frobenius algorithm for scalar multiplication on ECC against Differential Analysis. ρ is a random element of $\boldsymbol{Z}(\tau)$ and $N(\rho)$ denoted the norm of ρ in $\boldsymbol{Z}(\tau)$ where the length of (τ) -NAF is found approximately $m+\log_2(N(\rho))$. A few years later, Hedabou[7] replaced the multiplier k proposed by Joye and Tymen[6] with random element $k' \equiv k + r\frac{\tau^m - 1}{\tau - 1} \bmod \rho\,(\tau^m - 1)$ where r, ρ are a random elements of $Z(\tau)$ and $N(r)$ denoted as the norm of r in $\boldsymbol{Z}(\tau)$. Hedabou[7] also found that $N(r) \le N(\rho)$ and the length of τ-NAF expansion is only $m+\log_2(2\sqrt{N}) \approx m + \frac{\log_2(N(\rho))}{2} + 1$ for N equal to positive integers where the computational cost for this length is reduced for about 50 percent of the previous method proposed by Joye and Tymen[6]. Avanzi et al.[8] extended the work of τ-NAF with point halving by introducing a fast scalar multiplication called wide-double-NAF. Latest, Yunos et al.[9] continued to improve τ-NAF expansion by introducing formula of norm for every length in that expansion which is important in estimating the length of that expansion. Now, in this paper we analyze the norms of τ-NAF for every element in $\boldsymbol{Z}(\tau)$ in order to find the formulas for maximum and minimum norms where these maximum and minimum norms can help in estimating the length of τ-NAF expansion.

Below are several definitions collected from Solinas[4,5] and Yunos et al.[9] that we used in this study.

Definition 1: An element of the ring $Z(\tau)$ is represented as $r + s\tau$ where r and s are integers.

Definition 2: τ-adic non-adjacent form (τ-NAF) for some non-zero integers $\overline{n}$ which are elements of $Z(\tau)$ is defined as $\overline{n} = \sum_{i=0}^{l-1} c_i \tau^i$ with $c_i \in \{-1,0,1\}, c_{l-1} \neq 0,\ c_i c_{i+1} = 0$ and $l > 0$. The length of τ-NAF expansion is l.

Definition 3: Let $N : Z(\tau) \to Z$ be the norm function. Then, the norm $N(r+s\tau) = r^2 + trs + 2s^2$ where the trace $t = (-1)^{1-a}$.

Definition 4: Lucas sequence is a sequence of integers that can be used in calculation of irrational quadratic numbers. Lucas sequence is defined as follows:

$U_0 = 0, U_1 = 1$ and $U_\kappa = tU_{\kappa-1} - 2U_{\kappa-2}$ for $\kappa \ge 2$.

Before we give the property of norms of element in $Z(\tau)$, we would like to give the following table of short analysis of norms for τ-NAF with length-3 that was stated in Yunos et al.[9].

Table 1. Combinations of c_0, c_1 and c_2 and the norm of $c_0 + c_1\tau + c_2\tau^2$

C_2	C_1	C_0	t	r= C_0-2 C_2	s= C_1+ C_2t	N(r+s τ)
-1	0	-1	-1	1	1	2
-1	0	1	-1	3	1	8
-1	0	0	-1	2	1	4
-1	0	-1	1	1	-1	2
-1	0	1	1	3	-1	8
-1	0	0	1	2	-1	4
1	0	-1	-1	-3	-1	8
1	0	1	-1	-1	-1	2
1	0	0	-1	-2	-1	4
1	0	-1	1	-3	1	8
1	0	1	1	-1	1	2
1	0	0	1	-2	1	4

Based on the analysis of Table 1, we found that the maximum norm of τ -NAF expansion for length-3 is equal to 8 and the minimum norm of τ -NAF expansion for length-3 is equal to 2. Table 1 gives us the basic idea on how to obtained maximum and minimum norms for τ -NAF expansion those have certain length by analysing each norm for every integer in that length.

Solinas[5] denoted $N_{max}(l)$ as the largest norm occurring among all length elements of $Z(\tau)$ and $N_{min}(l)$ as the smallest norm occurring among all length elements of ( ) . Based on these $N_{max}(l)$ and $N_{min}(l)$, he derived the boundary for the norm of a length-l element as follows.

Theorem 1. Let $l > 2d$ and α be a length-l element of $Z(\tau)$, then

$$\left(\sqrt{N_{min}(d)} - \frac{\sqrt{N_{max}(d)}}{2^{\frac{d}{2}} - 1}\right)^2 2^{l-d} < N(\alpha) < \frac{N_{max}(d)}{(2^{\frac{d}{2}} - 1)^2} 2^l.$$

Based on the above theorem, Solinas[5] estimated that the length of the τ –NAF is bounded by

$$\log_2 N(\alpha) - 0.54626826939 < l < \log_2 N(\alpha) + 3.5155941234 \quad (1)$$

when $l > 30$. In order to achieve relation (1), $N_{max}(15) = 47324$ and $N_{max}(15) = 2996$ that obtained from direct evaluation method are applied in Theorem 1. The idea of direct evaluation method is acquired by Definition 4 in order to obtain the value of every norm $N(r+s\tau)$ for all integers in length-15 of τ-NAF are as follows.

$$\begin{aligned}
N(r+s\tau) &= N(c_0 + c_1\tau + c_2\tau^2 + c_3\tau^3 + c_4\tau^4 + c_5\tau^5 + \\
&\quad c_6\tau^6 + c_7\tau^7 + c_8\tau^8 + c_9\tau^9 + c_{10}\tau^{10} + \\
&\quad c_{11}\tau^{11} + c_{12}\tau^{12} + c_{13}\tau^{13} + c_{14}\tau^{14}) \\
&= N(c_0 + c_1\tau + c_2(U_2\tau - 2U_1) + c_3(U_3\tau - \\
&2U_2) + c_4(U_4\tau - 2U_3) + c_5(U_5\tau - 2U_4) + \\
&c_6(U_6\tau - 2U_5) + c_7(U_7\tau - 2U_6) + \\
&c_8(U_8\tau - 2U_7) + c_9(U_9\tau - 2U_8) + \\
&c_{10}(U_{10}\tau - 2U_9) + c_{11}(U_{11}\tau - 2U_{10}) + \\
&c_{12}(U_{12}\tau - 2U_{11}) + c_{13}(U_{13}\tau - 2U_{12}) + \\
&c_{14}(U_{14}\tau - 2U_{13})) \\
&= N(c_0 - 2c_2 - 2c_3 t + 2c_4 + 6c_5 t + 2c_6 - \\
&10c_7 t - 14c_8 + 6c_9 t + 34c_{10} + 22c_{11} t - \\
&46c_{12} - 90c_{13} t + 2c_{14} + (c_1 + c_2 t - c_3 - \\
&3c_4 t - c_5 + 5c_6 t + 7c_7 - 3c_8 t - 17c_9 - \\
&11c_{10} t + 23c_{11} + 45c_{12} t - c_{13} - 91c_{14} t)\tau)
\end{aligned}$$

where

$$r = c_0 - 2c_2 - 2c_3 t + 2c_4 + 6c_5 t + 2c_6 - 10c_7 t - 14c_8 + 6c_9 t + 34c_{10} + 22c_{11} t - 46c_{12} - 90c_{13} t + 2c_{14}$$

and

$$s = c_1 + c_2 t - c_3 - 3c_4 t - c_5 + 5c_6 t + 7c_7 - 3c_8 t - 17c_9 - 11c_{10} t + 23c_{11} + 45c_{12} t - c_{13} - 91c_{14} t.$$

By listing the value of all the norms $N(r+s\tau)$ consist in a certain length, Solinas[5] can determine the value of maximum and minimum norms for that length. A few years later, Yunos et al.[9] gave an alternative to the direct evaluation method by introducing the formula of norm $N(r+s\tau)$ in $Z(\tau)$ for every length-l that is

$$N(\sum_{i=0}^{l-1} c_i \tau^i) = (\sum_{i=0}^{l-1} c_i b_i t^i)^2 + t(\sum_{i=0}^{l-1} c_i b_i t^i)(\sum_{i=0}^{l-1} c_i a_i t^{i+1}) + 2(\sum_{i=0}^{l-1} c_i a_i t^{i+1})^2$$

where, $a_0 = 0, b_0 = 1, a_i = a_{i-1} + b_{i-1}$ and $b_i = -2a_{i-1}$. However, the direct evaluation method by Solinas[5] and the alternative formula produced by Yunos et al.[9] are not practically applicable for a large length where there are more than 43692 combination of $N(r+s\tau)$ that must be considered for length more than 15. Therefore, forming a formula to calculate maximum and minimum norms directly are important because we can estimate both maximum and minimum norms for any length. As mentioned in Solinas[5], the practical size of τ-NAF was at least 83. That is why we need to choose at least $d = 42$ to estimate the length of τ-NAF expansion. But the question now, is relation (1) still practical to be used to estimate the length for the case $l > 83$ or not? So in the next chapter, we will discuss in detail about this matter.

2. Result and Discussion

In this section, we discuss on how to obtain the formulas of maximum and minimum norms for τ-NAF occurring among all length element of $Z(\tau)$. Our study start with analysing the values of maximum and minimum norms of τ-NAF for length $l = 1,2,3,...,20$ as shown in the following table.

Table 2. Maximum and minimum norms of τ –NAF for length $l = 1,2,3,...,20$

l	Maximum norms	Minimum norms
1	1	1
2	2	2
3	8	2
4	16	4
5	37	7
6	81	9
7	162	18
8	352	28
9	704	56
10	1421	112
11	2921	197
12	5842	394
13	11816	764
14	23662	1498
15	47324	2996
16	94622	6058

17	189196	12188
18	378342	24442
19	756604	48980
20	1513102	988122

Based on Table 2, we can see that the values of maximum and minimum norms of τ-NAF are increase as the length increase. Other than that, we also found that the increment of maximum and minimum norms for every $l+1$ are about $2l$.

By making an analysis on the sequence of maximum norms as shown in Table 2, we found that

$N_{max}(l)$ = 11816, 23662, 47324, 94622, 189196, 378342, 756604, 1513102

for l = 13, 14, 15, 16, 17, 18, 19, 20 can be written as

$2^2(2954) + 0$, $2^2(5915) + 2$, $2^2(11831) + 0$, $2^2(23655) + 2$, $+2^2(47229) + 0$, $2^2(94585) + 0$, $2^2(189151) + 0$, $2^2(378275) + 2$.

Based on the above sequence, we obtain the following theorem.

Theorem 2. If $N_{max}(12) = 5842$ and

$$N_{max}(l) = 2N_{max}(l-1) + 2^2[5(14-(l-1)) + 2\sin\frac{(l-1)\pi}{2} - \cos\frac{(l-1)\pi}{2}] - 3\cos(l-1)\pi - 1,$$

then

$$N_{\max}(l) = 2^2\left[5(591\cdot 2^{l-13} + l - 13) - \sin\frac{l\pi}{2}\right] + 2\cos^2\frac{l\pi}{2} \quad (2)$$

for length $l \geq 13$.

Proof: This theorem has been proven by mathematical induction as follows.

If $l = 13$, then

$$N_{max}(13) = 11816$$

$$= 2(5842) + 32$$

$$= 2^2\left[5(591) - 1\right] + 0$$

$$= 2^2\left[5(591\cdot 2^0 + 0) - \sin\frac{13\pi}{2}\right] + 2\cos^2\frac{13\pi}{2}$$

$$= 2^2\left[5(591\cdot 2^{13-13} + 13 - 13) - \sin\frac{13\pi}{2}\right] + 2\cos^2\frac{13\pi}{2}.$$

So, relation (2) is true for $l = 13$.

Assume that if $l = k$ and

$$N_{\max}(k) = 2N_{\max}(k-1) + 2^2[5(14-(k-1)) + 2\sin\frac{(k-1)\pi}{2} - \cos\frac{(k-1)\pi}{2}] - 3\cos(k-1)\pi - 1,$$

then

$$N_{max}(k) = 2^2\left[5(591\cdot 2^{k-13} + k - 13) - \sin\frac{k\pi}{2}\right] + 2\cos^2\frac{k\pi}{2}$$

is true.

Now, for $l = k+1$,

$$N_{max}(k+1) = 2N_{max}(k) + 2^2[5(14-k) + 2\sin\frac{k\pi}{2} - \cos\frac{k\pi}{2}] - 3\cos k\pi - 1$$

$$= 2(2^2\left[5(591\cdot 2^{k-13} + k - 13) - \sin\frac{k\pi}{2}\right] + 2\cos^2\frac{k\pi}{2}) + 2^2[5(14-k) + 2\sin\frac{k\pi}{2} - \cos\frac{k\pi}{2}] - 3\cos 2(\frac{k\pi}{2}) - 1$$

$$= (1+1)(2^2\begin{bmatrix}5(591\cdot 2^{k-13} + k - 13)\\ -\sin\frac{k\pi}{2}\end{bmatrix} + 2\cos^2\frac{k\pi}{2}) + 2^2[5(14-k) + 2\sin\frac{k\pi}{2} - \cos\frac{k\pi}{2}] - 3\cos 2(\frac{k\pi}{2}) - 1$$

$$= 2^2[5(591\cdot 2^{k-13} + k - 13) - \sin\frac{k\pi}{2}] + 2\cos^2\frac{k\pi}{2} + 2^2[5(591\cdot 2^{k-13} + k - 13) - \sin\frac{k\pi}{2}] + 2\cos^2\frac{k\pi}{2} + 2^2[5(14-k) + 2\sin\frac{k\pi}{2} - \cos\frac{k\pi}{2}] - 3\cos 2(\frac{k\pi}{2}) - 1$$

$$= 2^2[5(591\cdot 2^{k-13} + k - 13) - \sin\frac{k\pi}{2}] + 2\cos^2\frac{k\pi}{2} + 2^2[5(591\cdot 2^{k-13} + k - 13 + 5(14-k) - \sin\frac{k\pi}{2} + 2\sin\frac{k\pi}{2} - \cos\frac{k\pi}{2} + [2\cos^2\frac{k\pi}{2} - 1] - 3[2\cos^2\frac{k\pi}{2} - 1]$$

$$=2^2[5\left(591\cdot 2^{k-13}+k-13\right)-\sin\frac{k\pi}{2}+2\cos^2\frac{k\pi}{2}+2^2[5(591\cdot 2^{k-13}+k-k+14-13+\left(2-1\right)\sin\frac{k\pi}{2}-\cos\frac{k\pi}{2}+(1-3)[2\cos^2\frac{k\pi}{2}-1]$$

$$=2^2[5\left(591\cdot 2^{k-13}+k-13\right)-\sin\frac{k\pi}{2}+2\cos^2\frac{k\pi}{2}+2^2[5(591\cdot 2^{k-13}+1)+\sin\frac{k\pi}{2}-\cos\frac{k\pi}{2}]-2[2\cos^2\frac{k\pi}{2}-1]$$

$$=2^2[5\left(591\cdot 2^{k-13}+k-13\right)-\sin\frac{k\pi}{2}]+2\cos^2\frac{k\pi}{2}+2^2[5(591\cdot 2^{k-13}+1)+\sin\frac{k\pi}{2}-\cos\frac{k\pi}{2}]-4\cos^2\frac{k\pi}{2}+2$$

$$=2^2[5\left(591\cdot 2^{k-13}+k-13\right)-\sin\frac{k\pi}{2}+2^2[5\left(591\cdot 2^{k-13}+1\right)+\sin\frac{k\pi}{2}-\cos\frac{k\pi}{2}]+2\cos^2\frac{k\pi}{2}-4\cos^2\frac{k\pi}{2}+2$$

$$=2^2[5\left(591\cdot 2^{k-13}+k-13\right)-\sin\frac{k\pi}{2}+5\left(591\cdot 2^{k-13}+1\right)+\sin\frac{k\pi}{2}-\cos\frac{k\pi}{2}]+(2-4)\cos^2\frac{k\pi}{2}+2$$

$$=2^2[5(591\cdot 2^{k-13}+591\cdot 2^{k-13}+k+1-13)-\sin\frac{k\pi}{2}+\sin\frac{k\pi}{2}-\cos\frac{k\pi}{2}]-2\cos^2\frac{k\pi}{2}+2$$

$$=2^2[5(591\cdot 2^1\cdot 2^{k-13}+k+1-13)-\cos\frac{k\pi}{2}+2\ [1-\cos^2\frac{k\pi}{2}]$$

$$=2^2[5\left(591\cdot 2^1\cdot 2^{k-13}+k+1-13\right)-\cos\frac{k\pi}{2}+2\sin^2\frac{k\pi}{2}$$

$$=2^2[5\left(591\cdot 2^1\cdot 2^{k-13}+k+1-13\right)-(\sin\frac{k\pi}{2}\cos\frac{\pi}{2}+\cos\frac{k\pi}{2}\sin\frac{\pi}{2})]+2[-\sin\frac{k\pi}{2}]^2$$

$$=2^2[5\left(591\cdot 2^1\cdot 2^{k-13}+k+1-13\right)-(\sin\frac{k\pi}{2}\cos\frac{\pi}{2}+\cos\frac{k\pi}{2}\sin\frac{\pi}{2})]+2[\cos\frac{k\pi}{2}\cos\frac{\pi}{2}-\sin\frac{k\pi}{2}\sin\frac{\pi}{2}]^2$$

$$=2^2[5\left(591\cdot 2^{k+1-13}+k+1-13\right)-\sin(\frac{k\pi}{2}+\frac{\pi}{2})]+2[\cos(\frac{k\pi}{2}+\frac{\pi}{2})]^2$$

$$=2^2[5\left(591\cdot 2^{k+1-13}+k+1-13\right)-\sin\frac{(k+1)\pi}{2}]+2\cos^2\frac{(k+1)\pi}{2}.$$

Therefore, relation (2) is still true for $l=k+1$ and will be true for all $l\geq 13$. □

Now, we analyze the sequence of minimum norms as shown in Table 2 and we found that

$N_{min}(l)=394,\ 764,\ 1498,\ 2996,\ 6058,\ 12188,\ 24442,\ 48980,\ 98122$

for $l=13,\ 14,\ 15,\ 16,\ 17,\ 18,\ 19,\ 20$ can be written as

$$2^3\left(95.5\right)+0,\ 2^3\left(187\right)+2,\ 2^3\left(374.5\right)+0,\ 2^3\left(757\right)+2,\ 2^3\left(1523.5\right)+0,\ 2^3\left(3055\right)+2,\ 2^3\left(6122.5\right)+0,\ 2^3(1225)+2\ .$$

Based on the above sequence, we obtain the following property.

Theorem 3. If $N_{min}\left(12\right)=394$ and

$$N_{\min}(l)=2N_{\min}(l-1)+2^3[3(\frac{1}{2}\cos\frac{(l-1)\pi}{2}-\sin\frac{(l-1)\pi}{2}+(l-1)-1)-37]-3\cos(l-1)\pi-1,$$

then

$$N_{\min}(l)=2^3\left[3\left(2^{l-8}-l+\frac{1}{2}\sin\frac{l\pi}{2}\right)+37\right]+2\cos^2\frac{l\pi}{2} \qquad (3)$$

for length $l\geq 13$.

Proof: This theorem has been proven by mathematical induction as follows.

If $l=13$, then

$$N_{min}\left(13\right)=764$$

$$=2\left(394\right)-24$$

$$= 2^3\left[3\left(2^5 - 13 + \frac{1}{2}\right) + 37\right] + 0$$

$$= 2^3\left[3\left(2^5 - 13 + \frac{1}{2}\sin\frac{13\pi}{2}\right) + 37\right] + 2\cos^2\frac{13\pi}{2}$$

$$= 2^3\left[3\left(2^{13-8} - 13 + \frac{1}{2}\sin\frac{13\pi}{2}\right) + 37\right] + 2\cos^2\frac{13\pi}{2}\ .$$

So, relation (3) is true for $l = 13$.

Assume that if $l = k$ and

$$N_{\min}(k) = 2N_{\min}(k-1) + 2^3\left[3\left(\frac{1}{2}\cos\frac{(k-1)\pi}{2} - \sin\frac{(k-1)\pi}{2} + (k-1) - 1\right) - 37\right] - 3\cos(k-1)\pi - 1$$

, then

$$N_{\min}(k) = 2^3\left[3\left(2^{k-8} - k + \frac{1}{2}\sin\frac{k\pi}{2}\right) + 37\right] + 2\cos^2\frac{k\pi}{2}$$

is true.

Now, for $l = k+1$,

$$N_{\min}(k+1) = 2N_{\min}(k) + 2^3\left[3\left(\frac{1}{2}\cos\frac{k\pi}{2} - \sin\frac{k\pi}{2} + k - 1\right) - 37\right] - 3\cos k\pi - 1$$

$$= 2N_{min}(k) + 2^3[3(\frac{1}{2}\cos\frac{k\pi}{2} - \sin\frac{k\pi}{2} + k - 1) - 37] - 3\cos 2\frac{k\pi}{2} - 1$$

$$= 2N_{\min}(k) + 2^3\left[3\left(\frac{1}{2}\cos\frac{k\pi}{2} - \sin\frac{k\pi}{2} + k - 1\right) - 37\right] - 3\left(2\cos^2\frac{k\pi}{2} - 1\right) - 1$$

$$= 2N_{\min}(k) + 2\ \ 3(\frac{}{2}\cos\frac{k\pi}{2} - \sin\frac{k\pi}{2} + k - 1) - 37] - 3\cdot 2\cos\ \ \text{——} + (3-1)$$

$$= 2N_{\min}(k) + 2^3[3(\frac{1}{2}\cos\frac{k\pi}{2} - \sin\frac{k\pi}{2} + k - 1) - 37] - 3\cdot 2\cos^2\frac{k\pi}{2} + 2$$

$$= 2\cdot(2^3\left[3\left(2^{k-8} - k + \frac{1}{2}\sin\frac{k\pi}{2}\right) + 37\right] + 2\cos^2\frac{k\pi}{2}) + 2^3[3(\frac{1}{2}\cos\frac{k\pi}{2} - \sin\frac{k\pi}{2} + k - 1) - 37] - 3\cdot 2\cos^2\frac{k\pi}{2} + 2$$

$$= (1+1)(2^3\left[3\left(2^{k-8} - k + \frac{1}{2}\sin\frac{k\pi}{2}\right) + 37\right] + 2\cos^2\frac{k\pi}{2}) + 2^3[3(\frac{1}{2}\cos\frac{k\pi}{2} - \sin\frac{k\pi}{2} + k - 1) - 37] - 3\cdot 2\cos^2\frac{k\pi}{2} + 2$$

$$= 2^3\left[3\left(2^{k-8} - k + \frac{1}{2}\sin\frac{k\pi}{2}\right) + 37\right] + 2\cos^2\frac{k\pi}{2} + 2^3\left[3\left(2^{k-8} - k + \frac{1}{2}\sin\frac{k\pi}{2}\right) + 37\right] + 2\cos^2\frac{k\pi}{2} + 2^3\left[3\left(\frac{1}{2}\cos\frac{k\pi}{2} - \sin\frac{k\pi}{2} + k - 1\right) - 37\right] - 3\cdot 2\cos^2\frac{k\pi}{2} + 2$$

$$= 2^3\left[3\left(2^{k-8} - k + \frac{1}{2}\sin\frac{k\pi}{2}\right) + 37\right] + 2\cos^2\frac{k\pi}{2} + 2^3[3(2^{k-8} - 1 - k + k + (\frac{1}{2} - 1)\sin\frac{k\pi}{2} + \frac{1}{2}\cos\frac{k\pi}{2}) + 37 - 37 + (-3+1)2\cos^2\frac{k\pi}{2} + 2$$

$$= 2^3\left[3\left(2^{k-8} - k + \frac{1}{2}\sin\frac{k\pi}{2}\right) + 37\right] + 2\cos^2\frac{k\pi}{2} + 2^3\cdot 3(2^{k-8} - 1 + \frac{1}{2}\cos\frac{k\pi}{2} - \frac{1}{2}\sin\frac{k\pi}{2}) - 2\cdot 2\cos^2\frac{k\pi}{2} + 2$$

$$= 2^3\left[3\left(2^{k-8} - k + \frac{1}{2}\sin\frac{k\pi}{2}\right) + 37\right] + 2\cos^2\frac{k\pi}{2} + 2^3\cdot 3(2^{k-8} - 1 + \frac{1}{2}\cos\frac{k\pi}{2} - \frac{1}{2}\sin\frac{k\pi}{2}) + 2(1 - 2\cos^2\frac{k\pi}{2})$$

$$= 2^3[3(2^{k-8} + 2^{k-8} - k - 1 + \frac{1}{2}\cos\frac{k\pi}{2} + \frac{1}{2}\sin\frac{k\pi}{2} - \frac{1}{2}\sin\frac{k\pi}{2}) + 37] + 2(1 - \cos^2\frac{k\pi}{2})$$

$$= 2^3\left[3\left(2^{k-8} + 2^{k-8} - k - 1 + \frac{1}{2}\cos\frac{k\pi}{2}\right) + 37\right] + 2\sin^2\frac{k\pi}{2}$$

$$= 2^3[3(2^{k-8} + 2^{k-8} - k - 1 + \frac{1}{2}(\sin\frac{k\pi}{2}\cos\frac{\pi}{2} + \cos\frac{k\pi}{2}\sin\frac{\pi}{2})) + 37] + 2(\cos\frac{k\pi}{2}\cos\frac{\pi}{2} - \sin\frac{k\pi}{2}\sin\frac{\pi}{2})^2$$

$$= 2^3\left[3\left(2\cdot 2^{k-8} - k - 1 + \frac{1}{2}\sin(\frac{k\pi}{2} + \frac{\pi}{2})\right) + 37\right] + 2\cos^2(\frac{k\pi}{2} + \frac{\pi}{2})$$

$$= 2^3\left[3\left(2^{k+1-8} - (k+1) + \frac{1}{2}\sin\frac{(k+1)\pi}{2}\right) + 37\right] + 2\cos^2\frac{(k+1)\pi}{2}.$$

Therefore, relation (3) is still true for $l = k+1$ and will be true for all $l \geq 13$. □

Now, we produce the following property of τ-NAF expansion for $l > 83$.

Theorem 4. Let length $l > 2d$, then length l of τ-NAF is bounded by

$$\log_2 N(\alpha) - 0.528943791 < l < \log_2 N(\alpha) + 3.415042901 \quad (4)$$

for $l > 83$.

Proof: We choose $d = 42$. By using Theorems 2 and 3 respectively, we obtained $N_{\max}(42) = 6.34581418 \times 10^{12}$ and $N_{min}(42) = 4.123168597 \times 10^{11}$. Now, by applying Theorem 1, we found that

$$\left(\sqrt{4.123168597 \times 10^{11}} - \frac{\sqrt{6.34581418 \times 10^{12}}}{2^{21} - 1}\right)^2 \cdot 2^{l-42} < N(\alpha) < \frac{6.34581418 \times 10^{12}}{(2^{21} - 1)^2} \cdot 2^l$$

$$0.093749649 \cdot 2^l < N(\alpha) < 1.44287247 \cdot 2^l$$

$$\log_2 N(\alpha) - 0.528943791 < l < \log_2 N(\alpha) + 3.415042901$$

for $l > 83$. □

By comparing relation (4) that has been produced with the relation (1), we found that the boundary of τ-NAF expansion is not same. As relation (4) is produced by obtaining $N_{max}(42)$ and $N_{min}(42)$ directly using Theorems 2 and 3 respectively, so definitely relation (4) is more accurate to use in estimating length of τ-NAF expansion for $l > 83$.

3. Conclusion

The maximum and minimum norms are used to determine the upper and lower bounds in order to estimate the length of τ-NAF expansion as we can see in Theorem 1. So, Theorems 2 and 3 that have been produced can be used to calculate the maximum and minimum norms directly for any length especially for $l > 83$. In future research, we extand this property to $l \geq 163$ since the standard size of the multiplier of scalar multiplication based on FIPS PUB 186-4 was at least 163.

4. References

1. Miller V. Use of elliptic curve in cryptography. Advance in Cryptology, Proc.Crypto'85, Proceedings Springer; 1986. p. 417–26.
2. Koblitz N. Elliptic curve cryptosystem. Mathematics Computation. 1987; 8(177):203–9.
3. Koblitz N. CM-curves with good cryptographic properties. Advance in Cryptology, Proc. Crypto'91, Springer; 1992. p. 279–87.
4. Solinas JA. An improved algorithm for arithmetic on a family of elliptic curves. Advance in Cryptology, Proc. CRYPTO'97, Springer; 1997. p. 357–71.
5. Solinas JA. Efficient arithmetic on Koblitz curves. Design, Codes, and Cryptography. 2000; 19:195–249.
6. Joye M, Tymen C. Protection against differential analysis for elliptic curve cryptography: an algebraic approach. Cryptography Hardware and Embedded Systems-CHES01, Springer; 2001. p. 377–90.

7. Hedabou M. A Frobenious map approach for an efficient and secure multiplication on Koblitz curves. International Journal of Network Security. 2006; 3(3):233–7.
8. Avanzi RM, Heuberger C, Prodinger H. Minimality of the Hamming weight of the $\hat{o}$-NAF for Koblitz curves and improved combination with point halving. Select-ed Areas in Cryptography, Springer Science & Business Media. 2006.
9. Yunos F, Atan MKA, Ariffin KMR, Said MMR. Pertanika Journal of Science & Technology. 2014; 22.
10. NIST [Internet]. [Cited 2013 Jul]. Available from: http:/nvl-pubs.nist.gov/nistpubs/FIPS/-NIST.FIPS. 186-4.pdf.