PROPERTIES OF PSEUDO t- ADIC NON-ADJACENT FORM AND THE EXPANSION OF t-ADIC NON-ADJACENT FORM

SYAHIRAH BINTI MOHD SUBERI

IPM 2018 16

PROPERTIES OF PSEUDO τ- ADIC NON-ADJACENT FORM AND THE EXPANSION OF τ-ADIC NON-ADJACENT FORM

By

SYAHIRAH BINTI MOHD SUBERI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

June 2017

DEDICATIONS

To my husband, Amir Hamzah bin Mohamad
and to my parents, Saripah Othman and Mohd Suberi Che Daud
for believing in me and not giving up on me
during my lowest
...

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

PROPERTIES OF PSEUDO τ- ADIC NON-ADJACENT FORM AND THE EXPANSION OF τ-ADIC NON-ADJACENT FORM

By

SYAHIRAH BINTI MOHD SUBERI

June 2017

Chairman : Faridah binti Yunos, PhD
Faculty : Institute for Mathematical Research

The elliptic curve cryptography (ECC) system are public key mechanisms where scalar multiplication (SM) is the dominant operation of ECC. SM is an operation involving the computation of an integer n for multiple n times with a point P on the Koblitz curve. In this research, the representation of the scalar n is in the form of pseudo τ-adic non-adjacent form (pseudoTNAF), that is $\sum_{i=0}^{l-1} c_i\tau^i$ of size $l > 0$ with $c_i \in \{-1,0,1\}$, $c_{l-1} \neq 0$ and $c_i c_{i+1} = 0$.

The objective of this research is to study some properties of $\rho_0 + \rho_1\tau$ in order to find the relation of n mod $(\rho_0 + \rho_1\tau)(\frac{\tau^m-1}{\tau-1})$ by considering three cases. Firstly, for the case when ρ_0 is odd and ρ_1 is even. Secondly, for ρ_0 is even and ρ_1 is odd and the last case is for both ρ_0 and ρ_1 are odd. From all these three cases, the behaviour of the scalar n is obtained and also we developed some properties for norm of $\rho_0 + \rho_1\tau$. As a result, the relation between the norms and the modulo congruence of $\bar{n} \equiv n$ mod $(\rho_0 + \rho_1\tau)\frac{\tau^m-1}{\tau-1}$ is obtained.

Besides, an algorithm is used in transforming TNAF expansion into an element of $\mathbb{Z}(\tau)$. By using the algorithm, we analyzed and construct the propositions regarding TNAF expansions having the least Hamming weight.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Sarjana Sains

CIRI BAGI PSEUDO τ-ADIC BUKAN-BERSEBELAHAN DAN KEMBANGAN τ-ADIC BUKAN-BERSEBELAHAN

Oleh

SYAHIRAH BINTI MOHD SUBERI

Jun 2017

Pengerusi : Faridah binti Yunos, PhD
Fakulti : Institut Penyelidikan Matematik

Sistem kriptografi lengkuk eliptik merupakan mekanisma kunci awam dengan pendaraban skalar adalah operasi paling dominan dalam sistem ini. Pendaraban skalar adalah suatu operasi yang melibatkan pengiraan integer n untuk n kali dengan suatu titik P di atas lengkuk Koblitz. Dalam kajian ini, perwakilan bagi skalar n adalah dalam bentuk pseudo τ-adic bukan-bersebelahan (pseudoTNAF) iaitu $\sum_{i=0}^{l-1} c_i \tau^i$ bersaiz $l > 0$ dengan $c_i \in \{-1, 0, 1\}$, $c_{l-1} \neq 0$ dan $c_i c_{i+1} = 0$.

Objektif kajian ini adalah untuk mengkaji ciri bagi $\rho_0 + \rho_1 \tau$ bagi tujuan untuk mencari kaitan bagi n mod $(\rho_0 + \rho_1 \tau)(\frac{\tau^m - 1}{\tau - 1})$ dengan mempertimbangkan tiga kes. Yang pertama, untuk kes apabila ρ_0 ganjil dan ρ_1 genap. Yang kedua, untuk ρ_0 genap dan ρ_1 ganjil dan kes yang terakhir untuk kedua-dua ρ_0 dan ρ_1 ganjil. Daripada ketiga-tiga kes, sifat pengganda n diperolehi dan kami juga membangunkan beberapa ciri bagi norma $\rho_0 + \rho_1 \tau$. Hasilnya, hubung kait di antara norma dan konguren modulo $\bar{n} \equiv n$ mod $(\rho_0 + \rho_1 \tau)(\frac{\tau^m - 1}{\tau - 1})$ diperolehi.

Selain itu, satu algoritma digunakan dalam mentransformasikan kembangan TNAF kepada suatu unsur dalam $\mathbb{Z}(\tau)$. Dengan menggunakan algoritma tersebut, kami menganalisis dan membina usulan berkaitan kembangan yang mempunyai pemberat Hamming yang kecil.

ACKNOWLEDGEMENTS

In the name of Allah, Most Gracious and Most Merciful. In praise of The Prophet SAW. Alhamdulillah, thankful to Allah for giving me the strength and health to do this research. Alhamdulillah, for having this opportunity to complete my Master.

I would like to express my gratitude to my supervisor Dr. Faridah binti Yunos for guiding and having the patience to help me through these two years. I would also like to thank Prof. Madya. Dr. Mohamad Rushdan bin Md. Said for helping me to go through this process.

Another big thanks to my husband, parents, and my family for sticking with me for whatever reasons. Last but not least, to my fellow friends, good luck and thank you so much!

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Faridah binti Yunos, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohamad Rushdan bin Md Said, PhD
Assosiate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

____

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature:______________________ Date:______________________

Name and Matric No: Syahirah binti Mohd Suberi, GS41040

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ____________________________

Name of Chairman of Supervisory Committee:

Dr. Faridah binti Yunos

Signature: ____________________________

Name of Member of Supervisory Committee:

Associate Professor Dr. Mohamad Rushdan bin Md Said

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

F_{2^m}	Binary field
ECC	Elliptic Curve Cryptography
SM	Scalar Multiplication
ECDLP	Elliptic Curve Discrete Logarithm Problem
τ	Frobenius mapping
$\mathbb{Z}(\tau)$	Polynomial ring over τ with its coefficients are integers
$\mathbb{Q}(\tau)$	Polynomial ring over τ with its coeffecients are rational
NAF	Non-Adjacent Form
TNAF	τ-Adic Non-Adjacent Form
RTNAF	Reduced τ-Adic Non-Adjacent Form
$\bar{\tau}$	Conjugate of $\tau : 1-\tau$
τ^2	$\tau^2 = t\tau - 1$
t	Trace for Frobenius mapping $\tau : E_a(F_{2^m}) \rightarrow E_a(F_{2^m})$
O	Point at infinity

CHAPTER 1

INTRODUCTION

1.1 Introduction

In this chapter, we give some terms and definitions that will be used in this research. Next, we will state the problem statement, research objectives and the organization of the thesis.

There are some terms that are commonly used in cryptography and definitions are listed as follows.

1) Plain text : the original message that will be transferred or stored.
2) Cipher text : the transformed original message.
3) Encryption : the process of converting the plain text to cipher text.
4) Decryption : the process of converting the cipher text to original message.
5) Secret key : numbers or sequence of integer numbers for encryption/decryption that are known to some party or parties that exchange plain text.
6) Public key : numbers or sequence of integer numbers that are publicly known.
7) Encryption key : secret key/public key that is used during the encryption process.
8) Decryption key : secret key/public key that is used during the decryption process.
9) Attacker: a third party(outsider) who wants to have the original message.
10) User: the person who has the access to the original message.

The following are some definitions from Koblitz (1987), Hankerson et al. (2006), Rosen (1993), Solinas (1997, 2000), Yunos et al.(2014, 2015, 2016), Ali and Yunos (2016) are used in our research.

Definition 1.1 : Koblitz curve is defined on F_{2^m} as follows

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

where $a \in \{0,1\}$.

Definition 1.2 : The Frobenius mapping of $\tau : E_a(F_{2^m}) \rightarrow E_a(F_{2^m})$ is defined by

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

where O is the point at infinity. The mapping satisfies $(\tau^2 + 2)(x,y) = t\tau(x,y)$ for all $(x,y) \in E_a(F_{2^m})$, where the trace, $t = (-1)^{1-a}$ and $a \in \{0,1\}$. It can be considered as a multiplication over complex number, $\tau = \frac{t+\sqrt{-7}}{2}$.

Definition 1.3 : An element of the ring $\mathbb{Z}(\tau)$ is represented as $r + s\tau$ where $r, s \in \mathbb{Z}$.

Definition 1.4 : A τ-adic Non-Adjacent Form (TNAF) of non zero $\bar{n}$ is defined as TNAF($\bar{n}$)=$\sum_{i=0}^{l-1} c_i\tau^i$ where l is the length of the expansion TNAF($\bar{n}$), $c_i \in \{-1,0,1\}$ and $c_ic_{i+1} = 0$.

Definition 1.5 : A Reduced τ-adic Non-Adjacent Form (RTNAF) of non zero $\bar{n}$ an element of $\mathbb{Z}(\tau)$ is defined as RTNAF($\bar{n}$)$\equiv \sum_{i=0}^{\bar{l}-1} c_i\tau^i$ modulo $(\frac{\tau^m-1}{\tau-1})$ where $\bar{l}$ is the length of the expansion RTNAF($\bar{n}$)$, c_i \in \{-1,0,1\}, c_{\bar{l}-1} \neq 0$ and $c_ic_{i+1} = 0$.

Definition 1.6 : A Pseudo τ-adic Non-Adjacent Form (pseudoTNAF) of non zero $\bar{n}$, an element of $\mathbb{Z}(\tau)$ is defined as pseudoTNAF($\bar{n}$) $\equiv \sum_{i=1}^{\bar{l}-1} c_i\tau^i$ modulo $\rho(\frac{\tau^m-1}{\tau-1})$ where $\bar{l}$ is the length of the expansion pseudoTNAF($\bar{n}$)$, \rho \in \mathbb{Z}(\tau), c_i \in \{-1,0,1\}, c_{\bar{l}-1} \neq 0$ and $c_ic_{i+1} = 0$.

Definition 1.7 : A Hamming Weight (HW) is defined as the number of coefficients 1 and -1 in an expansion of an element of $\mathbb{Z}(\tau)$.

Definition 1.8 : An operating cost is defined as the cost in terms of running time to calculate of the scalar multiplication of the number of doubling and addition operations on the Koblitz curve.

Definition 1.9 : A density among TNAF for an element of $\mathbb{Z}(\tau)$ having length l is defined as Hamming weight of the TNAF expansion divided by l.

Definition 1.10 : An average of Hamming weight among TNAF expansion for an element in $\mathbb{Z}(\tau)$ that having length l is defined as the Hamming weight among TNAF is devided by the number of combination of c_i and t where c_i is the coefficients of TNAF expansion and t is the trace of Frobenius endomorphism.

Definition 1.11 : An average density among TNAF for an element of $\mathbb{Z}(\tau)$ having length l is defined by as the average Hamming weight among TNAF is divided by the length l.

Definition 1.12 : Let m be a positive integer. If a and b are integers, we say that a is congruent to b modulo m if $m|(a-b)$. If a is congruent to b modulo m, we write $a \equiv b$ (mod m) and say that a and b incongruent modulo m.

Definition 1.13 : The norm of $\alpha = r + s\tau \in \mathbb{Z}(\tau)$ is the integer product of α and its complex conjugate $\bar{\alpha}$. Explicitly,

$$N(r+s\tau) = r^2 + trs + 2s^2$$

where the trace $t = (-1)^{(1-a)}$.

1.2 Mathematical Background

In this subsection, we discuss some introduction of Elliptic Scalar Multiplication (ECC), τ-adic Non-Adjacent Form (TNAF), Reduced τ-adic Non-Adjacent Form (RTNAF) and Koblitz Curve.

1.2.1 Elliptic Scalar Multiplication

Elliptic curve has different kinds of forms. In this research, we focus on the curve over F_{2^m} known as the Koblitz curve (Koblitz (1987)) defined as

$$E_a(F_{2^m}) : y^2 + xy = x^3 + ax^2 + b \tag{1.1}$$

where $a \in \{0,1\}$ and $b = 1$.

The sets of point (x,y) that satisfy equation (1.1) are the points on the elliptic curve.

Scalar multiplication (SM) involved computing integer for multiple times for a scalar n and a point P denoted as $nP = P + P + ... + P$ for n times such that $nP = Q$ where P and Q are points on the elliptic curve. Elliptic Curve Discrete Logarithm Problem (ECDLP) is the problem of determining the value of n when P and Q were given. Security systems based on elliptic curve cryptography (ECC) rely on the hardness of these ECDLP. When computing SM, nP, n is referred as the secret key and have different powers of τ. For example, TNAF expansion of 25, TNAF(25) $= [1,0,0,1,0,0,-1,0,0,-1,0,0,-1]$. It is also can be written as $25 = -\tau^{12} - \tau^9 - \tau^6 + \tau^3 + 1$. Since complex multiplication property is useful for elliptic scalar multiplication by τ, being implemented by squaring is free. If $P = (x,y)$ is a point on the Koblitz curve then

$$25P = -(x^{4096}, y^{4096}) - (x^{512}, y^{512}) - (x^{64}, y^{64}) + (x^8, y^8) + (x,y)$$

Scalar multiplication can be achieved by addition and doubling operation.

1. Point addition : Let $G = (x_1, y_1)$, $H = (x_2, y_2)$ and $R = (x_3, y_3)$ are points on $E_a(F_{2^m})$. Point addition is the operation of adding two points of G and H to obtain a new point (written as $G + H = R$). There are three cases for the addition of points G and H.

   i) First case is for $G \neq \pm H$. For this case, $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$, $y_3 = \lambda(x_1 + x_3) + x_3 + y_1$, and $\lambda = \frac{y_1+y_2}{x_1+x_2}$ where a is one of the parameter choosed based on the elliptic curve, E_a and λ is the gradient of the line that passes the point G to H.

   ii) The second case is for $H = -G$ where $H = (x_1, x_1 + y_1)$, then the addition of G and H results in O (written as $G + H = O$).

   iii) The third case is for $H = G$. Then $G + H = 2G$ by using the concept of doubling. Besides that, since all the elements in $E_a(F_{2^m})$ satisfy the commutative property, then $H + G = G + H$.

   Figure 1.1 explains the point addition of G and H.

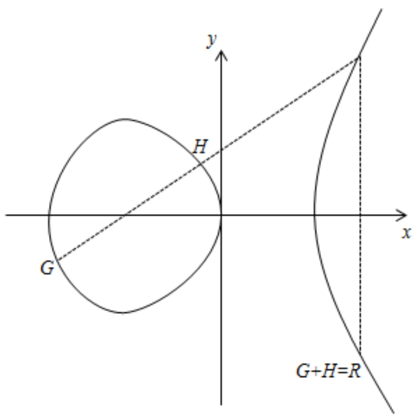

Figure 1.1: Point Addition of *G* and *H*

2. Point doubling : This operation involves adding a point G to itself having $2G$ written as $R = 2G$. Consider point $G = (x_1, y_1)$ with $y_1 \neq 0$. Let $R = 2G$ with $R = (x_3, y_3)$ then $x_3 = \lambda^2 + \lambda + a$, $y_3 = {x_1}^2 + \lambda(x_3 + 1)$, and $\lambda = x_1 + \frac{y_1}{x_1}$ with λ is the tangent from the point G and a is one of the parameter choosen based on the elliptic curve. Figure 1.2 explains the point doubling geometrically.

1.2.2 Koblitz Curve

Koblitz curves are also known as the Anomalous Binary Curves (ABC) defined over $\mathbb{F}_2$. Solinas (2000) introduced TNAF where it is one of the efficient algorithms to calculate the scalar multiplication. We give a few basic properties of the Koblitz curves based on Solinas (2000) and Hankerson et al. (2006).

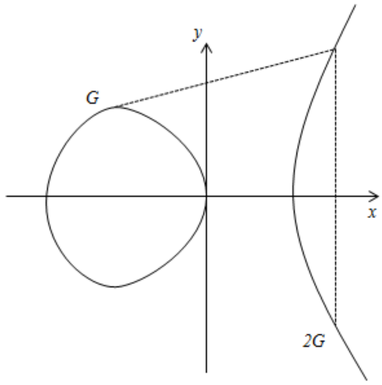

Figure 1.2: Point Doubling of G

1. Group orders: The group order of $\mathbb{F}_{2^m}$ is denoted by $E_a(\mathbb{F}_{2^m})$ where it is the points on the extension field $\mathbb{F}_{2^m}$. Group $\mathbb{F}_{2^m}$ is choosen to perform the encryption and decryption process. The group order $\#E_a(\mathbb{F}_{2^m})$ is a prime or a product of a prime with small integer. $\#E_a(\mathbb{F}_{2^m}) = gh$ where h is prime and $g = 4$ if $a = 0$ or $g = 2$ if $a = 1$. h is prime when m is prime. One of the criteria to perform the process by choosing a prime m.

2. Complex Multiplication: Since the Koblitz curves are defined over $\mathbb{F}_{2^m}$, they have the following properties.

   i) If $P = (x,y)$ is a point on E_a then so is the point (x^2, y^2). Besides, it is proven that
   $$(x^4, y^4) + 2(x,y) = t \cdot (x^2, y^2)$$
   for every (x,y) on E_a.

   ii) Let τ refer to Frobenius endomorphism. Frobenius mapping $\tau : E_a(F_{2^m}) \mapsto E_a(F_{2^m})$ for point $P = (x,y)$ on $E_a(F_{2^m})$ defined by
   $$\tau(x,y) = (x^2, y^2), \tau(\mathscr{O}) = \mathscr{O}$$
   with $\mathscr{O}$ point at infinity.

   iii) If $(\tau^2 + 2)P = t\tau P$ for all $P \in E_a(F_{2^m})$, with the trace, $t = (-1)^{1-a}$. Therefore E_a has complex multiplication with the number $\tau = \frac{t+\sqrt{-7}}{2}$.

3. Lucas sequence: Lucas sequence are the sequences of integers that will help in computations involving quadratic irrationals. We summarize the relevant properties as follows:

   i) There are two Lucas sequences U_i and V_i, defined by:
   $$U_0 = 0, U_1 = 1 \text{ and } U_i = tU_{i-1} - 2U_{i-2} \text{ for } i \geq 2;$$
   $$V_0 = 2, V_1 = t \text{ and } V_i = tV_{i-1} - 2V_{i-2} \text{ for } i \geq 2.$$

ii) It has been proved

$$U_i = \frac{\tau^i - \bar{\tau}^i}{\sqrt{-7}};$$
$$V_i = \tau^i + \bar{\tau}^i.$$

4. Norm: the norm of an element $\alpha \in \mathbb{Z}(\tau)$ is the product of α and its conjugate $\bar{\alpha}$. The norm of $\alpha = \alpha_1 + \alpha_2\tau$ is $N(\alpha) = {\alpha_1}^2 + t\alpha_1\alpha_2 + 2{\alpha_2}^2$. The following are the properties of norm.

   i) 1 and -1 are the only elements of $\mathbb{Z}(\tau)$ having norm 1.
   ii) $N(\tau) = 2$ and $N(\tau - 1) = h$ for $h = 4$ if $a = 0$ or $h = 2$ if $a = 1$ whereby a is a parameter choose for Koblitz curve.
   iii) The norm function is multiplicative; that is $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$ for all α_1 and α_2 are element of $\mathbb{Z}(\tau)$.

1.2.3 τ-adic Non-Adjacent Form

For any $\alpha = c + d\tau$ an element of $\mathbb{Z}(\tau)$ it can be written as $\alpha = \sum_{i=0}^{l-1} c_i\tau^i$ for every $c_i \in \{-1, 0, 1\}$. The following theorem discuss the properties of τ-adic Non-Adjacent Form (TNAF).

Theorem 1.1 *: Let* $\alpha \in \mathbb{Z}(\tau)$ and $\alpha \neq 0$ then

(i) TNAF(α) is a unique digit representation.

(ii) If the length $l(\alpha)$ is greater than 30, then

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

where $N(\alpha)$ is the norm of α.

iii) The average density of non zero digits in the expansion of l is approximately $\frac{1}{3}$.

TNAF representation of α can be written as TNAF(α) $= [c_0, c_1, c_2, ..., c_{l-2}, c_{l-1}]$. The coefficients, c_i of TNAF are generated by repeatedly dividing α with τ such that c and d are equal to 0. If α is not divisible by τ then it can have the remainder, $c_i \in \{-1, 1\}$ so that the quotient $\frac{\alpha - c_i}{\tau}$ is divisible by τ. The next coefficient, c_{i+1} of TNAF expansion should have the value 0 since $c_ic_{i+1} = 0$. We show the example of finding TNAF(25) where $\alpha = 25 + 0\tau$, $c = 25, d = 0, a = 1$ and $\bar{\tau} = 1 - \tau$ is the conjugate of τ. First, we show that $\tau \cdot \bar{\tau} = 2$.

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

We proceed with the steps in obtaining TNAF(25).

Step 1: Since 25 is not divisible by τ, we choose $c_0 = 1$. The remainder can either be 1 or -1. Since the next coefficient must be 0, c_0 is 1 so that $c_i c_{i+1} = 0$.

$$\begin{aligned}\frac{25-1}{\tau} &= \frac{24}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}}\\ &= \frac{24\cdot\bar{\tau}}{2}\\ &= 12\cdot\bar{\tau}\\ &= 12(1-\tau)\\ &= 12-12\tau.\end{aligned}$$

Therefore, TNAF(25)$= [1, c_1, c_2, ..., c_{l-1}]$.

Step 2: Since $12-12\tau$ is divisible by τ, then $c_1 = 0$.

$$\begin{aligned}\frac{12-12\tau}{\tau} &= \frac{12}{\tau} - 12\\ &= \frac{12}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}} - 12\\ &= \frac{12\cdot\bar{\tau}}{2} - 12\\ &= 6\cdot\bar{\tau} - 12\\ &= 6(1-\tau) - 12\\ &= -6-6\tau.\end{aligned}$$

Thus, TNAF(25)$= [1, 0, c_2, ..., c_{l-1}]$.

Step 3: Since $-6-6\tau$ is divisible by τ, then $c_2 = 0$.

$$\begin{aligned}\frac{-6-6\tau}{\tau} &= \frac{-6}{\tau} - 6\\ &= \frac{-6}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}} - 6\\ &= \frac{-6\cdot\bar{\tau}}{2} - 6\\ &= -3\cdot\bar{\tau} - 6\\ &= -3(1-\tau) - 6\\ &= -9+3\tau.\end{aligned}$$

Thus, TNAF(25)$= [1,0,0,c_3,...,c_{l-1}]$.

Step 4: Since $-9+3\tau$ is not divisible by τ, then $c_3 = 1$.

$$\begin{aligned}\frac{-8+3\tau-1}{\tau} &= \frac{-10}{\tau}+3\\ &= \frac{-10}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}}+3\\ &= \frac{-10\cdot\bar{\tau}}{2}+3\\ &= -5\bar{\tau}+3\\ &= -5(1-\tau)+3\\ &= -2+5\tau.\end{aligned}$$

Thus, TNAF(25)$= [1,0,0,1,c_4,...,c_{l-1}]$.

Step 5: Since $-2+5\tau$ is divisible by τ, then $c_4 = 0$.

$$\begin{aligned}\frac{-2+5\tau}{\tau} &= \frac{-2}{\tau}+5\\ &= \frac{-2}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}}+5\\ &= \frac{-2\cdot\bar{\tau}}{2}+5\\ &= -\bar{\tau}+5\\ &= -1+\tau+5\\ &= 4+\tau.\end{aligned}$$

Thus, TNAF(25)$= [1,0,0,1,0,c_5,...,c_{l-1}]$.

Step 6: Since $4+\tau$ is divisible by τ, then $c_5 = 0$.

$$\begin{aligned}\frac{4+\tau}{\tau} &= \frac{4}{\tau}+1\\ &= \frac{4}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}}+1\\ &= \frac{4\cdot\bar{\tau}}{2}+1\\ &= 2\cdot\bar{\tau}+1\\ &= 2(1-\tau)+1\\ &= 3-2\tau.\end{aligned}$$

Thus, TNAF(25)= $[1,0,0,1,0,0,c_6,...,c_{l-1}]$.

Step 7: Since $3-2\tau$ is not divisible by τ, we choose the next coefficient $c_6 = -1$.

$$\begin{aligned}\frac{3-2\tau-(-1)}{\tau} &= \frac{4}{\tau}-2\\ &= \frac{4}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}}-2\\ &= \frac{4\cdot\bar{\tau}}{2}-2\\ &= 2\cdot\bar{\tau}-2\\ &= 2(1-\tau)-2\\ &= 2-2\tau-2\\ &= -2\tau.\end{aligned}$$

Thus, TNAF(25)= $[1,0,0,1,0,0,-1,c_7,...,c_{l-1}]$.

Step 8: Since -2τ is divisible by τ, then $c_7 = 0$.

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

Thus, TNAF(25)= $[1,0,0,1,0,0,-1,0,c_8,...,c_{l-1}]$.

Step 9: Since -2 is divisible by τ, then $c_8 = 0$.

$$\begin{aligned}\frac{-2}{\tau} &= \frac{-2}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}}\\ &= \frac{2\cdot\bar{\tau}}{2}\\ &= \bar{\tau}\\ &= 1-\tau.\end{aligned}$$

Thus, TNAF(25)= $[1,0,0,1,0,0,-1,0,0,c_9,...,c_{l-1}]$.

Step 10: Since $1-\tau$ is not divisible by τ, we choose $c_9 = -1$.

$$\begin{aligned}
\frac{1+\tau-(-1)}{\tau} &= \frac{2+\tau}{\tau} \\
&= \frac{2+\tau}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} + 1 \\
&= \frac{2 \cdot \bar{\tau}}{2} + 1 \\
&= \bar{\tau} + 1 \\
&= 1 - \tau + 1 \\
&= 2 - \tau.
\end{aligned}$$

Thus, TNAF(25)= $[1,0,0,1,0,0,-1,0,0,-1,c_{10},...,c_{l-1}]$.

Step 11: Since $2-\tau$ is divisible by τ, then $c_{10} = 0$.

$$\begin{aligned}
\frac{2-\tau}{\tau} &= \frac{2}{\tau} - 1 \\
&= \frac{2}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} - 1 \\
&= \frac{2 \cdot \bar{\tau}}{2} - 1 \\
&= \bar{\tau} - 1 \\
&= 1 - \tau - 1 \\
&= -\tau.
\end{aligned}$$

Thus, TNAF(25)= $[1,0,0,1,0,0,-1,0,0,-1,0,c_{11},...,c_{l-1}]$.

Step 12: Since $-\tau$ is divisible by τ, therefore $c_{11} = 0$.

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

Thus, TNAF(25)= $[1,0,0,1,0,0,-1,0,0,-1,0,0,c_{12},...,c_{l-1}]$.

Step 13: Since -1 is not divisible by τ, then we choose $c_{12} = -1$.

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

Thus, TNAF(25)= $[1,0,0,1,0,0,-1,0,0,-1,0,0,-1]$.

It is also can be written as $25 = -\tau^{12} - \tau^9 - \tau^6 + \tau^3 + 1$. We use the concept of division of an integer 25 with τ in obtaining the expansion of TNAF (25). It is much more efficient by using the following Lemma 1.1 that given by Solinas(1997).

Lemma 1.1 : Let $\alpha = c + d\tau \in \mathbb{Z}(\tau)$.

(i) α is divisible by τ if and only if c is even. That is

$$\frac{\alpha}{\tau} = (d + \frac{tc}{2}) - (\frac{c}{2})\tau \tag{1.2}$$

where t is a parameter that is chosen. If c is not even, then the remainder is chosen between 1 or -1.

(ii) α is divisible by τ^2 if and only if $c \equiv 2d \pmod 4$.

Based on Lemma 1.1, Solinas(1997) developed an algorithm for finding TNAF expansion of α as shown in Algorithm 1.1.

Algorithm 1.1 :(TNAF)

Input : *integers* c, d;
Output : $TNAF(c + d\tau)$;
Computation :

```
Set c0 ← c, c1 ← d
Set S ← ⟨⟩
While c0 ≠ 0 or c1 ≠ 0
   If c0 odd then
       set u ← 2 − (c0 − 2c1 mod 4)
       set c0 ← c0 − u
   else
       set u ← 0
   Prepend u to S
       Set (c0, c1) ← (c1 + tc0/2, −c0/2)
End While
Output S
```

This algorithm has also been used by Yunos et al. (2015) in constructing the programming as shown as in Figure 1.3.

We choose the parameter $a = 0, c_0 = 25$ and $c_1 = 0$. By using Algorithm 1.1, we obtain TNAF(25)= $[1,0,0,1,0,0,-1,0,0,-1,0,0,-1]$ and the length of the expansion, (l) is 13 and the density, (d) is $\frac{5}{13}$ respectively. This algorithm also can be used to find TNAF expansion for integers, $1 \leqslant n \leqslant 21$.

```
a := can be either 0 or 1;
t := (-1)^(1-a);
c[0] := any integer;
c[1] := any integer;
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·c[1];
        d := convert(f, rational);
        e := modp(d, 4);
        v[i] := 2 - e;
        c := c - v[i];
    else
        v[i] := 0
    end if;
    R := c[0];
    c[0] := c[1] + tc[0]/2;
    c[1] := -R/2;
    i := i + 1;
    j := i;
end do;
TNAF := seq(v[i], i = 0...j-1);
LengthTNAF := nops(TNAF);
NonzeroCoefficientForTNAF := remove(has, TNAF, 0);
HammingWeightTNAF := nops(NonzeroCoefficientForTNAF);
If LengthTNAF <> 0 then
    Density := HammingWeightTNAF / LengthTNAF;
end if;
DensityTNAF := convert(Density, float, 5);
```

Figure 1.3: Programming for Algorithm 1.1

1.2.4 Reduced τ-adic Non-Adjacent Form

Reduced τ-adic Non-Adjacent Form (RTNAF) is another form of TNAF expansion. RTNAF is an expansion of non zero element, $\bar{n}$ of $\mathbb{Z}(\tau)$, written as $\bar{n}$ where RTNAF($\bar{n}$)$\equiv \sum_{i=0}^{\bar{l}-1} c_i \tau^i$ modulo $(\frac{\tau^m - 1}{\tau - 1})$. $\bar{l}$ is the length of the expansion RTNAF($\bar{n}$), $c_i \in \{-1, 0, 1\}, c_{\bar{l}-1} \neq 0$, $c_i c_{i+1} = 0$ and m is a prime number. The expression of $(\frac{\tau^m - 1}{\tau - 1})$ is first transformed into $r + s\tau \in \mathbb{Z}(\tau)$ by using Lucas sequence. Then the modular reduction is performed by division and rounding off operation (refer to Routine 74 in Solinas(2000)) using the following algorithms. The steps of finding the expansion RTNAF's are similar as finding TNAF's expansion.

Algorithm 1.2: Rounding off Algorithm

Input : *rational numbers* λ_0, *and* λ_1;
Output : *integers x and y such that* $x + y\tau$ *is closed to the complex numbers* $\lambda_0 + \lambda_1\tau$;
Computation :

1. For i from 0 to 1 do
   1.1 $f_i \leftarrow floor(\lambda_i + \frac{1}{2})$.
   1.2 $\eta_i \leftarrow \lambda_i - f_i$.
   1.3 $h_i \leftarrow 0$.
2. $\eta \leftarrow 2\eta_0 + t\eta_1$.
3. If $\eta \geq 1$ then
   3.1 If $\eta_0 - 3t\eta_1 < -1$ then $h_1 \leftarrow t$; else $h_0 \leftarrow 1$
   else
   3.2 If $\eta_0 + 4t\eta_1 \geq 2$ then $h_1 \leftarrow t$.
   set $u \leftarrow 2 - (c_0 - 2c_1 \bmod 4)$
   set $u \leftarrow 2 - (c_0 - 2c_1 \bmod 4)$
4. If $\eta < -1$ then
   4.1 If $\eta_0 - 3t\eta_1 \geq 1$ then $h_1 \leftarrow -t$; else $h_0 \leftarrow -1$
   else
   4.2 If $\eta_0 + 4t\eta_1 < -2$ then $h_1 \leftarrow -t$.
5. $x \leftarrow f_0 + h_0, y \leftarrow f_1 + h_1$.
6. Return to (x, y)

Algorithm 1.3: Division in Ring of $\mathbb{Z}(\tau)$

Input : dividend $a + b\tau$ *and divisor* $c + d\tau \neq 0$.
Output: quotient $x + y\tau$ *and the remainder* $w + z\tau$.
Computation :

Set $k \leftarrow ac + tad + 2ad$,
$l \leftarrow bc - ad$
Set $N \leftarrow c^2 + tcd + 2d^2$
Set $\lambda_0 \leftarrow \frac{k}{N}$,
$\lambda_1 \leftarrow \frac{l}{N}$
Use Algorithm 2.2 to calculate $(x, y) \leftarrow Round(\lambda_0, \lambda_1)$
Set $w \leftarrow a - cx + 2dy$,
$z \leftarrow b - dx - cy - tdy$
Output x, y, w, z

Both of the Rounding off Algorithm and the Division Algorithm are used in the process of division in $\mathbb{Z}(\tau)$. The output $x + y\tau$ is the final product of these two algorithms where it is the result of modular reduction integer n. These two algorithms are used in Chapter 3 to find $\bar{n}$ such that $\bar{n} \equiv n \bmod (f + e\tau)$.

1.3 Problem Statement

The RTNAF and pseudoTNAF systems have approximately been equivalent operating cost as TNAF. The average density among TNAF, RTNAF, and pseudoTNAF for an element of $\mathbb{Z}(\tau)$ is approximately $\frac{1}{3}$.

Yunos et al. (2015) has proposed two properties for $\rho = \rho_1 + \rho_2\tau$ where $\bar{n} \equiv \bar{n} \bmod \rho\frac{\tau^m-1}{\tau-1}$. Based on these two traits, it can be used to predict the output of the transformation of $\rho\frac{\tau^m-1}{\tau-1}$. The first property is when ρ_0 is even and the second property is when both ρ_0 and ρ_1 are even. It gives us an idea to expand the properties of ρ_0 and ρ_1. We will consider the properties of ρ for $\bar{n} \equiv \bar{n} \bmod \rho(\tau^m-1)$ and $\bar{n} \equiv \bar{n} \bmod \rho\frac{\tau^m-1}{\tau-1}$.

Solinas in 1997 has introduced the TNAF expansion of $\bar{n} = r + s\tau$ for an element of $\mathbb{Z}(\tau)$ and can be written as TNAF($\bar{n}$) $= \sum_{i=0}^{l-1} c_i\tau^i$ or TNAF($\bar{n} = [c_0, c_1, c_2, \ldots, c_{l-2}, c_{l-1}]$) for l is the length of the expansion and $c_i \in \{-1, 0, 1\}$. We focus on the three cases of the first coefficient, c_0 of TNAF expansion. By developing an algorithm for the transformation of the TNAF expansion into an element of $\mathbb{Z}(\tau)$, we identify TNAF expansions having the least number of Hamming weight, (HW). Having smaller number of HW means the TNAF expansion have small operational cost.

1.4 Research Objective

The objectives of this research are as follows:

1. To develop several properties of ρ in the ring of $\mathbb{Z}(\tau)$ in the form of pseudoTNAF expansion. The properties of ρ affect the selection of n of the multiplier SM.

2. To find a new approach to predict value of n of the multiplier SM.

3. To find a general form of TNAF expansion having small number of Hamming weight indirectly have low operation cost.

1.5 Organization of Thesis

In Chapter 2, we give the mathematical background of elliptic scalar multiplication, τ-adic non adjacent form, reduced τ-adic non adjacent form, pseudo τ-adic non adjacent form and the koblitz curve. We also give the literature review that is related to this project.

In Chapter 3, we give three properties regarding ρ. The first case is where ρ_0 is odd and ρ_1 is even, the second case is where ρ_0 is even and ρ_1 is odd and the third case is where ρ_0 and ρ_1 are odd. We also provide proof for each cases. Then, we give some properties regarding the norm of an element in $\mathbb{Z}(\tau)$. The three properties are important in understanding the behaviour of n_1 and n_2 when using $\bar{n} \equiv n_1 + n_2\tau \bmod \rho(\tau^m - 1)$ and $\bar{n} \equiv n_1 + n_2\tau \bmod \rho(\frac{\tau^m - 1}{\tau - 1})$.

In Chapter 4, we identify cases for integers that have differerent values for c_0 for TNAF expansion where c_0 can have the values -1, 0 or 1. Then we proceed to the TNAF expansion that have the least number of Hamming weight. The last chapter is where the conclusion are made and the future research is proposed.

REFERENCES

Ali, N. A. and Yunos, F. (2016). Maximum and minimum norms for τ-naf expansion on koblitz curve. *Indian Journal of Science and Technology*, 9(28).

Ali, N. A., Yunos, F., Jamal, N. H., Kilicman, A., Srivastava, H. M., Mursaleen, M., and Khalique, C. M. (2017). A total norm of τ-adic non-adjacent form occurring among all element of (τ): An alternative formula. In *AIP Conference Proceedings*, volume 1795, page 020002. AIP Publishing.

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. In *International Workshop on Selected Areas in Cryptography*, pages 332–344. Springer.

Brumley, B. B. and Järvinen, K. (2007). Koblitz curves and integer equivalents of frobenius expansions. In *International Workshop on Selected Areas in Cryptography*, pages 126–137. Springer.

Hankerson, D., Menezes, A. J., and Vanstone, S. (2006). *Guide to Elliptic Curve Cryptography*. Springer Science & Business Media.

Heuberger, C. and Mazzoli, M. (2014). Symmetric digit sets for elliptic curve scalar multiplication without precomputation. *Theoretical computer science*, 547:18–33.

Jedwab, J. and Mitchell, C. J. (1989). Minimum weight modified signed-digit representations and fast exponentiation. *Electronics Letters*, 25(17):1171–1172.

Joye, M. and Tymen, C. (2001). Protections against differential analysis for elliptic curve cryptography - an algebraic approach. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 377–390. Springer.

Knuth, D. (1968). The art of computer programming 1: Fundamental algorithms 2: Seminumerical algorithms 3: Sorting and searching. *MA: Addison-Wesley*, page 30.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209.

Li, M., Qin, B., Kong, F., and Li, D. (2007). Wide-w-naf method for scalar multiplication on koblitz curves. In *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on*, volume 2, pages 143–148. IEEE.

Lin, T. C. (2007). Algorithms on elliptic curves over fields of characteristic two with non-adjacent forms. 9(2):117–120.

Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 417–426. Springer.

Rosen, K. H. (1993). *Elementary number theory and its applications*. Addison-Wesley.

Solinas, J. A. (1997). An improved algorithm for arithmetic on a family of elliptic curves. In *Annual International Cryptology Conference*, pages 357–371. Springer.

Solinas, J. A. (2000). Efficient arithmetic on koblitz curves. *Designs, Codes and Cryptography*, 19(2-3):195–249.

Yunos, F. (2015). *PseudoTNAF Representation for Scalar Multiplication on Koblitz Curve*. PhD thesis, Institute for Mathematical Research, Universiti Putra Malaysia.

Yunos, F., Atan, K. A. M., Ariffin, M. R. K., and Said, M. R. M. (2014). A reduced τ-adic naf (rtnaf) representation for an efficient scalar multiplication on anomalous binary curves (abc). *Pertanika Journal of Science & Technology*, 22(2):489–505.

Yunos, F., Atan, K. A. M., Ariffin, M. R. K., and Said, M. R. M. (2015). Pseudo τ-adic non adjacent form for scalar multiplication on koblitz curves. *Malaysian Journal of Mathematical Sciences*, 9(spec.):71–88.

Yunos, F., Atan, K. A. M., Salleh, S., Aris, N., Bahar, A., Zainuddin, Z. M., Maan, N., Lee, M. H., Ahmad, T., and Yusof, Y. M. (2016). Improvement to scalar multiplication on koblitz curves by using pseudo τ-adic non-adjacent form. In *AIP Conference Proceedings*, volume 1750, page 050006. AIP Publishing.