UNIVERSITI PUTRA MALAYSIA

KEMBANGAN PSEUDOTNAF UNTUK PENDARABAN SKALAR DI ATAS LENKUK KOBLITZ

FARIDAH YUNOS

GSM 2014 8

KEMBANGAN PSEUDOTNAF UNTUK PENDARABAN SKALAR DI ATAS LENGKUK KOBLITZ

Oleh

FARIDAH BINTI YUNOS

Tesis Dikemukakan Kepada Sekolah Pengajian Siswazah, Universiti Putra Malaysia, Sebagai Memenuhi Keperluan Untuk Ijazah Doktor Falsafah

November 2014

HAK CIPTA

DEDIKASI

Khas untuk perwira hatiku Mohd Hanizzan Bin Mohd Hanafiah yang telah banyak memberi dorongan dan sokongan moral sehingga selesainya tesis ini. Juga tidak dilupakan kepada ibu Safiah Binti Marjan yang sentiasa memanjatkan doa kehadrat Illahi tidak mengira siang ataupun malam agar anaknya ini sentiasa tabah dalam mengharungi cabaran dan dugaan yang mendatang. Tidak dilupai budi kedua ibubapa mertuaku yang menjadi pemangkin kejayaanku. Untuk permata hati ibu, Ainan Farhani, Mohd Imran dan Irdina Sofia, jadikanlah ilmu ini sebagai harta warisan yang tak ternilai harganya.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

KEMBANGAN PSEUDOTNAF UNTUK PENDARABAN SKALAR DI ATAS LENGKUK KOBLITZ

Oleh

FARIDAH BINTI YUNOS

November 2014

Pengerusi: Prof. Dato' Kamel Ariffin Bin Mohd Atan, Ph.D.
Institut: Penyelidikan Matematik

Sistem Kriptografi Lengkuk Eliptik telah dipiawaikan sebagai sistem kriptografi yang lebih praktikal digunakan selain daripada Sistem Kriptografi Rivest, Shamir dan Adleman. Dalam sistem ini, pendaraban skalar merupakan operasi yang dominan iaitu pengiraan gandaan integer untuk suatu integer dan suatu titik yang berada di atas lengkuk elips. Pada tahun 1997, Solinas telah memperkenalkan kembangan berbentuk τ-adic bukan-bersebelahan (τ-NAF) untuk suatu integer bukan sifar $\bar{n}$ unsur dalam gelanggang $Z(\tau)$. Ianya merupakan kembangan

$$\bar{n} = \sum_{i=0}^{l-1} c_i \tau^i$$

bersaiz $l > 0$ dengan $c_i \in \{-1, 0, 1\}$, $c_{l-1} \neq 0$ dan $c_i c_{i+1} = 0$. Algoritma yang dihasilkan oleh beliau adalah salah satu algoritma yang paling berkesan untuk mengira pendaraban skalar di atas lengkuk Koblitz

$$E_a\left(F_{2^m}\right) : y^2 + xy = x^3 + ax^2 + 1$$

dengan nombor perdana $m > 2$, $a \in \{0, 1\}$ dan titik $x, y \in F_{2^m}$. Ianya dapat menghapuskan operasi penggandaan eliptik dan mengekalkan operasi penambahan dalam pendaraban skalar $\bar{n}P$ di atas lengkuk ini. Ini disebabkan oleh kos operasi untuk melaksanakan pemetaan Frobenius

$$\tau : E_a\left(F_{2^m}\right) \mapsto E_a\left(F_{2^m}\right)$$

yang mematuhi hubungan $(\tau^2 - 2)(x, y) = t\tau(x, y)$ dengan surihan $t = (-1)^{1-a}$, $\tau(x, y) = \left(x^2, y^2\right)$ dan $\tau(\mathcal{O}) = \mathcal{O}$ ($\mathcal{O}$ adalah titik pada ketakterhinggaan) adalah

pada dasarnya percuma. Pada tahun 2000, Solinas dapat mengekalkan keadaan ini dengan menggantikan suatu integer yang berbentuk τ-NAF kepada suatu kembangan berbentuk τ-NAF terturunkan. Dalam penyelidikan ini, satu lagi ungkapan yang setara dengan τ-NAF diperolehi yakni pseudo τ-adic bukan-bersebelahan (pseudoTNAF) untuk suatu integer bukan sifar $\bar{n}$ bermodulo $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$ unsur dalam $Z(\tau)$ yang merupakan kembangan

$$\bar{n} = \sum_{i=0}^{\bar{l}-1} c_i \tau^i$$

bersaiz $\bar{l} > 0$ dengan $\rho \in Z(\tau)$, $c_i \in \{-1, 0, 1\}$, $c_{\bar{l}-1} \neq 0$ dan $c_i c_{i+1} = 0$. Kami telah membuktikan bahawa τ-NAF bagi dua elemen dalam Z(τ) adalah setara iaitu, jika $\gamma, \beta \in Z(\tau)$ dengan

$$\gamma \equiv \beta \; mod \; \rho\frac{\tau^m - 1}{\tau - 1}$$

maka $\gamma P = \beta P$ untuk semua $P \in E_a(F_{2^m})$. Oleh yang demikian, kami dapat membina algoritma pendaraban yang hampir setara dengan algoritma τ-NAF yang asal dari segi kos operasi eliptiknya.

Kos operasi pseudoTNAF hanya bergantung kepada bilangan operasi penambahan yang berasaskan kos purata pemberat Hammingnya (iaitu bilangan pekali-pekali bukan sifar) yang bersaiz $\bar{l} > 30$. Purata ini adalah hasil daripada pendaraban antara purata ketumpatan di kalangan kembangannya yang bersaiz $\bar{l} > 30$ dan panjang maksimumnya apabila $\bar{l} > 30$. Bagi tujuan untuk menganggarkan kos operasi ini, maka analisis terhadap bilangan cara menyusun pekali-pekali -1 dan 1 dan surihan t ke atas kembangan τ-NAF yang asal yang bersaiz 1 sehinggalah 15 dibuat menerusi gambarajah pokok. Kita memperolehi formula norma untuk kembangan $\sum_{i=0}^{l-1} c_i \tau^i$. Formula ini digunakan untuk menentukan norma maksimum ($N_{max}(l)$) dan minimum ($N_{min}(l)$) dalam kalangan τ-NAF bersaiz l suatu integer dalam $Z(\tau)$.

Kajian kami dapat menjangkakan panjang maksimum pseudoTNAF bersaiz $\bar{l} > 30$ (yakni $log_2 N(\rho) + m + a$) berpandukan $N_{max}(15)$ dan $N_{min}(15)$. Purata ketumpatan pekali bukan sifar dalam kembangan pseudoTNAF bersaiz $\bar{l} > 30$ (yakni $\approx \frac{1}{3} + o(1)$) pula diperolehi melalui formula purata ketumpatan pekali bukan sifar dalam kalangan τ-NAF bersaiz $l > 30$. Purata pemberat Hamming pseudoTNAF dapat dianggarkan menggunakan hasil darab di antara $\frac{1}{3} + o(1)$ dan $log_2 N(\rho) + m + a$. Berdasarkan anggaran purata ini, kajian kami telah membuktikan bahawa kos operasi untuk mengira pseudoTNAF adalah setara dengan τ-NAF dan τ-NAF terturunkan.

Bagi tujuan untuk mendapatkan integer pengganda yang mempunyai pemberat

Hamming terendah dalam kalangan semua titik yang bermodulo $r + s\tau$ dengan $r, s \in Z$, titik-titik kekisi yang berada dalam persilangan set Z dan $(r + s\tau)Z(\tau)$ dikenalpasti. Jika ungkapan $r+s\tau$ tersebut boleh difaktorkan kepada $\rho^{'}\left(r^{'} + s^{'}\tau\right)$ maka titik-titik kekisi tersebut adalah ahli kepada set $\rho^{'}N(r^{'}+s^{'}\tau)Z$ dan bilangannya sebanyak $\left|\rho^{'}\right| N(r^{'} + s^{'}\tau)$. Kami turut memperkenalkan suatu algoritma untuk mendapatkan titik-titik kekisi tersebut. Ini adalah bertujuan untuk mempercepatkan proses untuk mendapatkan integer pengganda yang sesuai dan memastikan integer yang dicari tidak melebihi peringkat bagi titik P. Untuk memastikan proses pendaraban skalar tidak menuju ketakterhinggaan, maka diberikan syarat tambahan bagi integer tadi iaitu $N(\bar{n}) \leq \frac{4}{7}N(\rho\frac{\tau^m-1}{\tau-1})$ dan dalam masa yang sama $N(\rho) \geq \frac{7N(n)}{4N(\frac{\tau^m-1}{\tau-1})}$.

Kita turut mengkaji dua sifat bagi ρ yang membahagi sebarang elemen dalam $Z(\tau)$ yang boleh mempengaruhi pemilihan integer pengganda iaitu pertamanya untuk kes ρ_0 genap dan keduanya untuk kes ρ_0 dan ρ_1 genap. Kita juga menggunakan semula dua algoritma yang telah diperkenalkan oleh Solinas (2000) yakni algoritma pembahagian elemen dalam $Z(\tau)$ dan algoritma untuk mendapatkan kembangan τ-NAF suatu elemen dalam $Z(\tau)$ dalam algoritma pendaraban skalar dengan pseudoTNAF.

Terdapat satu kelebihan yang ketara bagi algoritma kajian kami jika dibandingkan dengan algoritma pendaraban skalar yang dibina oleh Solinas dalam tahun 1997 dan 2000. Yakni, disediakan algoritma berorientasikan jujukan Lucas untuk mempercepatkan proses pendaraban dua elemen yang berada dalam $Z(\tau)$ sebagai langkah awal sebelum pembahagian elemen dalam $Z(\tau)$. Di akhir kajian ini, kita telah membuktikan bahawa kaedah pseudoTNAF lebih berkesan daripada kaedah τ-NAF dan RTNAF dengan pemilihan ρ yang sesuai. Oleh yang demikian, kaedah yang kami bangunkan boleh dijadikan alternatif kepada kedua-dua kaedah tadi dan boleh diaplikasikan ke dalam sistem kriptologi.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

PSEUDOTNAF REPRESENTATION FOR SCALAR MULTIPLICATION ON KOBLITZ CURVE

By

FARIDAH BINTI YUNOS

November 2014

Chair: Prof. Dato' Kamel Ariffin Bin Mohd Atan, Ph.D.
Institute: Mathematical Research

Elliptic Curve Cryptosystem was standardized as a more practical cryptographic system used instead of Rivest, Shamir and Adleman Cryptosystems. In this system, the scalar multiplication is the dominant operation of computing integer multiple for an integer and a point on an elliptic curve. In year 1997, Solinas introduced the expansion of the form τ-adic non- adjacent (τ-NAF) for a non-zero element $\bar{n}$ in the ring $Z(\tau)$. This is an expansion

$$\bar{n} = \sum_{i=0}^{l-1} c_i \tau^i$$

of size $l > 0$ with $c_i \in \{-1, 0, 1\}$, $c_{l-1} \neq 0$ and $c_i c_{i+1} = 0$.The algorithm developed by him is one of the most efficient algorithm to compute the scalar multiplication on Koblitz curve

$$E_a\left(F_{2^m}\right) : y^2 + xy = x^3 + ax^2 + 1$$

with a prime number $m > 2$, $a \in \{0, 1\}$ and a point $x, y \in F_{2^m}$. It can eliminate the elliptic doublings in scalar multiplication $\bar{n}P$ method on this curve, and double the number of elliptic additions. This is due to the operating costs for implementing the Frobenius mapping

$$\tau : E_a\left(F_{2^m}\right) \mapsto E_a\left(F_{2^m}\right)$$

which satisfying the relation $(\tau^2 - 2)(x, y) = t\tau(x, y)$ with the trace $t = (-1)^{1-a}$, $\tau(x, y) = \left(x^2, y^2\right)$ and $\tau(\mathcal{O}) = \mathcal{O}$ ($\mathcal{O}$ is a point at infinity) is basically free. In year 2000, Solinas was able to maintain this situation by replacing an integer in the form of τ-NAF with an expansion of the form reduced τ-NAF. In this research, another expression equivalent to τ-NAF obtained i.e. pseudo τ-adic non-adjacent

(pseudoTNAF) for a non-zero integer $\bar{n}$ modulo $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$ an element of $Z(\tau)$. That is, an expansion

$$\bar{n} = \sum_{i=0}^{\bar{l}-1} c_i \tau^i$$

of size $\bar{l} > 0$ with $\rho \in Z(\tau)$, $c_i \in \{-1, 0, 1\}$, $c_{\bar{l}-1} \neq 0$ and $c_i c_{i+1} = 0$. We proved that τ-NAF of two elements in Z(τ) are equivalent. That is, if $\gamma, \beta \in Z(\tau)$ with

$$\gamma \equiv \beta \; mod \; \rho \frac{\tau^m - 1}{\tau - 1}$$

then $\gamma P = \beta P$ for all $P \in E_a(F_{2^m})$. Therefore, we can build a multiplication algorithm that is almost equivalent to the original τ-NAF in terms of the elliptic operational costs.

The operating costs of pseudoTNAF only depends on the number of addition operations based on the average cost of the Hamming weights (i.e. the number of non-zero coefficients) of size $\bar{l} > 30$. Such average is a product of average density among its expansion of size $\bar{l} > 30$ with the maximum length when $\bar{l} > 30$. For the purpose of estimating the cost of this operation, the analysis of the number of arrangements for all coefficients -1 and 1 and trace t made on the original τ-NAF of size 1 until 15 by using tree diagram. We obtain a formula for the norm of $\sum_{i=0}^{l-1} c_i \tau^i$ expansion. This formula is used in determining the maximum norm ($N_{max}(l)$) and the minimum norm ($N_{min}(l)$) among τ-NAF of size l an integer in $Z(\tau)$.

In our study, we can produce a maximum length of pseudoTNAF of size $\bar{l} > 30$ (i.e. $log_2 N(\rho) + m + a$) based on $N_{max}(15)$ dan $N_{min}(15)$. The average density of non-zero coefficients among pseudoTNAF expansion of $\bar{l} > 30$ (i.e. $\approx \frac{1}{3} + o(1)$) was obtained by the formula of average density of non-zero coefficients among the τ-NAF of the length $l > 30$. The average of Hamming weights can be estimated by using the product of $\frac{1}{3} + o(1)$ and $log_2 N(\rho) + m + a$. Based on this estimation, our study has shown that the operating costs of the scalar multiplication algorithm with pseudoTNAF is equivalent to τ-NAF and reduced τ-NAF.

In order to find the integer multiplier that has the lowest Hamming weight among all points in modulo $r + s\tau$ with $r, s \in Z$, all lattice points that was in the intersection set between Z and $(r + s\tau)Z(\tau)$ was identified. If the expression $r + s\tau$ can be factored into $\rho'\left(r' + s'\tau\right)$ then the lattice points are element of the set $\rho' N(r' + s'\tau)Z$ where its cardinality is $\left|\rho'\right| N(r' + s'\tau)$. We also introduce an algorithm to obtain the lattice points. It is intended to accelerate the process for obtaining the appropriate multiplier and to ensure such integer does not exceed the order of the point P. To ensure that there are no scalar multiplication

process towards infinity, then the additional conditions for the integer that is $N(\bar{n}) \leq \frac{4}{7}N(\rho\frac{\tau^m-1}{\tau-1})$ was given and at the same time $N(\rho) \geq \frac{7N(n)}{4N(\frac{\tau^m-1}{\tau-1})}$.

We also examine two properties of ρ that divides any element in $Z(\tau)$ which can influence the selection of the integer multiplier. Firstly, for the case ρ_0 is an even and secondly, for both of ρ_0 and ρ_1 are even. We also reused two algorithms that have been introduced by Solinas (2000) in the scalar multiplication with pseudoTNAF. There are, the algorithm for elements division in $Z(\tau)$ and the algorithm to get the expansion of τ-NAF an element of $Z(\tau)$.

There is a significant advantage of our algorithm compared to the scalar multiplication algorithms which were constructed by Solinas in 1997 and 2000. Thus, it is an algorithm based on Lucas sequence to speed up the process of multiplication of two elements of $Z(\tau)$ as a preliminary step before the division of an elements of $Z(\tau)$. At the end of this study, we have shown that the pseudoTNAF is more efficient than the τ-NAF and RTNAF methods by choosing an appropriate ρ. Therefore, the scalar multiplication algorithm with pseudoTNAF can be used as an alternative to both of these methods and it can be applied to cryptosystems.

PENGHARGAAN

Segala pujian dan sanjungan untuk Allah, Tuhan seru sekalian alam ini. Alhamdulillah, dengan limpah rahmat-Nya penulis dapat menyempurnakan kajian ini. Juga, selawat dan salam ke atas junjungan besar Nabi Muhammad (S.A.W).

Jutaan terima kasih diucapkan kepada Pengerusi Jawatankuasa Penyeliaan iaitu Prof. Dato' Dr. Kamel Ariffin Bin Mohd Atan atas segala kesabaran, dorongan dan bimbingan beliau selama beberapa tahun ini. Ucapan terima kasih yang tak terhingga diberikan kepada Prof. Madya Dr. Mohamad Rushdan Bin Md Said dan juga Prof. Madya Dr. Muhammad Rezal Bin Kamel Ariffin selaku Jawatankuasa Penasihat yang turut memberikan idea di awal kajian ini.

Tidak lupa kepada rakan-rakan daripada Jabatan Matematik, Universiti Putra Malaysia yang memberikan dorongan secara tak langsung. Akhir sekali, ingatan buat ibu yang sentiasa mendoakan anaknya di sini.

Tesis ini telah dikemukakan kepada Senat Universiti Putra Malaysia dan telah diterima sebagai memenuhi syarat keperluan untuk ijazah **Doktor Falsafah**. Ahli Jawatankuasa Penyeliaan adalah seperti berikut:

Dato' Hj. Kamel Ariffin Bin Mohd. Atan, Ph.D.
Profesor
Institut Penyelidikan Matematik
Universiti Putra Malaysia
(Pengerusi)

Muhammad Rezal Bin Kamel Ariffin, Ph.D.
Profesor Madya
Institut Penyelidikan Matematik
Universiti Putra Malaysia
(Ahli)

Mohamad Rushdan Bin Md Said, Ph.D.
Profesor Madya
Institut Penyelidikan Matematik
Universiti Putra Malaysia
(Ahli)

BUJANG KIM HUAT, Ph.D.
Profesor dan Dekan
Sekolah Pengajian Siswazah
Universiti Putra Malaysia

Tarikh:

Perakuan pelajar siswazah

Saya memperakui bahawa:

- tesis ini adalah hasil kerja saya yang asli;
- setiap petikan, kutipan dan ilustrasi telah dinyatakan sumbernya dengan jelas;
- tesis ini tidak pernah dimajukan sebelum ini, dan tidak dimajukan serentak dengan ini, untuk ijazah lain sama ada di Universiti Putra Malaysia atau di institusi lain;
- hak milik intelek dan hakcipta tesis ini adalah hak milik mutlak Universiti Putra Malaysia, mengikut Kaedah-Kaedah Universiti Putra Malaysia (Penyelidikan) 2012;
- kebenaran bertulis daripada penyelia dan Pejabat Timbalan Naib Canselor (Penyelidikan dan Inovasi) hendaklah diperoleh sebelum tesis ini diterbitkan (dalam bentuk bertulis, cetakan atau elektronik) termasuk buku, jurnal, modul, prosiding, tulisan popular, kertas seminar, manuskrip, poster, laporan, nota kuliah, modul pembelajaran atau material lain seperti yang dinyatakan dalam Kaedah-Kaedah Universiti Putra Malaysia (Penyelidikan) 2012;
- tiada plagiat atau pemalsuan/fabrikasi data dalam tesis ini, dan integriti ilmiah telah dipatuhi mengikut Kaedah-Kaedah Universiti Putra Malaysia (Pengajian Siswazah) 2003 (Semakan 2012-2013) dan Kaedah-Kaedah Universiti Putra Malaysia (Penyelidikan) 2012. Tesis telah diimbaskan dengan perisian pengesanan plagiat.

Tandatangan:_____ Tarikh: **24/3/2015**

Nama dan No. Matrik: **FARIDAH BINTI YUNOS (GS 23207)**

Perakuan Ahli Jawatankuasa Penyeliaan

Dengan ini, diperakukan bahawa:

- penyelidikan dan penulisan tesis ini adalah di bawah seliaan kami;
- tanggungjawab penyeliaan sebagaimana yang dinyatakan dalam Kaedah- Kaedah Universiti Putra Malaysia (Pengajian Siswazah) 2003 (Semakan 2012- 2013) telah dipatuhi.

Tandatangan: _____
Nama Pengerusi **HAJI KAMEL**
Jawatankuasa **ARIFFIN BIN**
Penyeliaan: **MOHD ATAN**

Tandatangan: _____
Nama Ahli **MUHAMMAD**
Jawatankuasa **REZAL BIN KAMEL**
Penyeliaan: **ARIFFIN**

Tandatangan: _____
Nama Ahli **MOHAMAD**
Jawatankuasa **RUSHDAN BIN**
Penyeliaan: **MD SAID**

JADUAL KANDUNGAN

SENARAI JADUAL

SENARAI RAJAH

SENARAI SIMBOL DAN SINGKATAN

$AVGHW_l$	Purata pemberat Hamming bagi τ-NAF semua unsur dalam $Z(\tau)$ yang mempunyai panjang-l
$AVGDensity_l$	Purata bagi pekali-pekali bukan sifar c_i untuk setiap panjang-l
ECC	Kriptografi Lengkuk Eliptik
F_q	Medan terhingga berperingkat q
F_{q^m}	Medan terhingga berperingkat q^m
F_{2^m}	Medan dedua
$Z(\tau)$	Gelanggang polinomial dalam sebutan τ dengan pekali-pekalinya adalah integer
$\mathbb{Q}(\tau)$	Gelanggang polinomial dalam sebutan τ dengan pekali-pekalinya adalah nisbah
HW_l	Pemberat Hamming bagi unsur bukan sifar yang terjadi dalam kalangan kembangan τ-NAF bagi semua unsur dalam $Z(\tau)$ yang mempunyai panjang-l
lim	had
$\bar{n}$, ρ, r_{hed}	Suatu elemen dalam $Z(\tau)$
NAF	Bentuk Bukan-Bersebelahan
NAF_l	Kembangan NAF yang bersaiz l
τ-NAF	Bentuk τ-Adic Bukan-Bersebelahan
$TNAF_l$	Kembangan τ-NAF yang bersaiz l
$N_{max}(d)$	Norma maksimum yang terjadi dalam kalangan kembangan τ-NAF bagi semua unsur dalam $Z(\tau)$ yang mempunyai panjang-d
$N_{min}(d)$	Norma minimum yang terjadi dalam kalangan kembangan τ-NAF bagi semua unsur dalam $Z(\tau)$ yang mempunyai panjang-d
RTNAF	Bentuk τ-Adic Bukan-Bersebelahan Terturunkan
PseudoTNAF	Bentuk Pseudo τ-Adic Bukan-Bersebelahan
RSA	Rivest Shamir Adleman
t	Surihan bagi pemetaan Frobenius $\tau : E_a(F_{2^m}) \rightarrow E_a(F_{2^m})$
t'	Surihan bagi lengkuk eliptik E di atas F_q
$\Bbbk$	Kecerunan pada suatu titik di atas Lengkuk Eliptik dalam medan F_{2^m}

BAB 1

PENGENALAN

1.1 Beberapa Istilah dan Takrif

Di dalam penulisan tesis ini, beberapa istilah yang biasa digunakan dalam sistem kriptografi digunapakai dan diperjelaskan maksudnya seperti berikut:

1) Teks asal :mesej yang akan diubah oleh pengutus mesej kepada bentuk mesej rahsia.

2) Teks saifer :teks rahsia yang akan diutuskan kepada penerima mesej.

3) Pengkriptanan :proses menukarkan teks asal kepada teks saifer.

4) Penghuraian :proses menukarkan teks saifer kepada teks asal.

5) Kunci rahsia :nombor atau jujukan nombor-nombor integer yang dirahsiakan daripada pengetahuan umum.

6) Kunci awam :nombor atau jujukan nombor-nombor integer yang diketahui umum.

7) Kunci pengkriptan :kunci rahsia/awam yang diaplikasikan semasa proses pengkriptanan.

8) Kunci penghurai :kunci rahsia/awam yang diaplikasikan semasa proses penghuraian.

Berikut merupakan beberapa takrif yang digunakan dalam kajian kami.

Takrif 1.1 : Lengkuk Koblitz ditakrifkan di atas F_{2^m} seperti berikut:

$$E_a : y^2 + xy = x^3 + ax^2 + 1 \tag{1.1}$$

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

Takrif 1.2 : Pemetaan Frobenius $\tau : E_a(F_{2^m}) \mapsto E_a(F_{2^m})$ untuk titik (x, y) di atas $E_a(F_{2^m})$ ditakrifkan oleh

$$\tau(x, y) = \left(x^2, y^2\right), \quad \tau(\mathcal{O}) = \mathcal{O} \tag{1.2}$$

dengan $\mathcal{O}$ titik pada ketakterhinggaan. Pemetaan Frobenius ini mematuhi perkaitan $(\tau^2 - 2)(x, y) = t\tau(x, y)$ dengan surihan $t = (-1)^{1-a}$ dan $a \in \{0, 1\}$.

Takrif 1.3 : Bentuk Bukan-Bersebelahan (NAF) untuk suatu integer positif n merupakan kembangan

$$n = \sum_{i=0}^{l-1} c_i 2^i \tag{1.3}$$

dengan $c_i \in \{-1, 0, 1\}$, $c_{l-1} \neq 0$, $c_i c_{i+1} = 0$ dan $l > 0$. Panjang kembangan NAF ialah l.

Takrif 1.4 : Suatu integer dalam gelanggang $Z(\tau)$ boleh dituliskan sebagai $r + s\tau$ dengan r dan s suatu integer.

Takrif 1.5 : Bentuk τ-adic Bukan-Bersebelahan (τ-NAF) untuk suatu integer bukan sifar $\bar{n}$ unsur dalam $Z(\tau)$ merupakan kembangan

$$\bar{n} = \sum_{i=0}^{l-1} c_i \tau^i \tag{1.4}$$

dengan $c_i \in \{-1, 0, 1\}$, $c_{l-1} \neq 0$, $c_i c_{i+1} = 0$ dan $l > 0$. l ialah panjang kembangan τ-NAF.

Takrif 1.6 : Bentuk pseudo τ-adic Bukan-Bersebelahan (pseudoTNAF) untuk suatu integer bukan sifar $\bar{n}$ unsur dalam $Z(\tau)$ merupakan kembangan

$$\bar{n} = \sum_{i=0}^{\bar{l}-1} c_i \tau^i \tag{1.5}$$

bermodulo $\rho\left(\frac{\tau^m - 1}{\tau - 1}\right)$ dengan $\rho \in Z(\tau)$, $c_i \in \{-1, 0, 1\}$, $c_{\bar{l}-1} \neq 0$, $c_i c_{i+1} = 0$ dan $\bar{l} > 0$. $\bar{l}$ ialah panjang kembangan pseudoTNAF.

Takrif 1.7 : Pemberat Hamming ditakrifkan sebagai bilangan pekali-pekali -1 dan 1 dalam kembangan suatu unsur dalam $Z(\tau)$.

Takrif 1.8 : Katakan $N : \mathbb{Q}(\tau) \to \mathbb{Q}$ fungsi norma. Jika $\alpha = x + y\tau$ suatu unsur dalam $\mathbb{Q}(\tau)$ dengan $x, y \in \mathbb{Q}$ maka normanya ialah

$$N(\alpha) = x^2 + txy + 2y^2 \tag{1.6}$$

dengan $t = (-1)^{1-a}$ dan $a \in \{0, 1\}$.

Takrif 1.9 : Kos pengiraan operasi ditakrifkan sebagai kos dari sudut masa larian untuk mengira pendaraban skalar iaitu bilangan operasi penggandaan dan operasi penambahan.

Takrif 1.10 : Fungsi surihan di atas F_{2^m} adalah fungsi $Tr : F_{2^m} \to F_{2^m}$ dengan $Tr(x) = x^2$ ditakrifkan sebagai

$$Tr(x) = \sum_{i=0}^{m-1} x^{2^i}. \tag{1.7}$$

Takrif 1.11 : Medan F_{2^m} yang dipersembahkan dalam sebutan asas normal adalah suatu asas di atas F_2 dalam bentuk $\{ \tau, \tau^2, \tau^{2^2}, \ldots, \tau^{2^{2^{m-1}}} \}$.

Takrif 1.12 : Purata pemberat Hamming dalam kalangan τ-*NAF* bagi semua ahli-ahli dalam $Z(\tau)$ yang mempunyai panjang-l ditakrifkan sebagai pemberat Hamming dalam kalangan τ-NAF tersebut dibahagikan dengan bilangan kombinasi c_i dan t.

Takrif 1.13 : Purata ketumpatan dalam kalangan τ-NAF bagi semua ahli-ahli dalam $Z(\tau)$ yang mempunyai panjang-l ditakrifkan sebagai purata pemberat Hamming dalam kalangan τ-NAF tersebut dibahagikan dengan panjang l.

Takrif 1.14 : Purata pemberat Hamming dalam kalangan pseudoTNAF bagi semua ahli-ahli dalam $Z(\tau)$ yang mempunyai panjang-$\bar{l}$ ditakrifkan sebagai purata ketumpatan dalam kalangan kembangannya didarabkan dengan panjang maksimumnya apabila $\bar{l} > 30$.

Takrif 1.15 : Setiap integer bukan sifar n boleh diwakilkan dengan asas 2 secara unik, seperti berikut:

$$n = \sum_{i=0}^{j} e_i 2^i \tag{1.8}$$

dengan $e_i \in \{-1, 0, 1\}$ dan $e_j \neq 0$. Kembangan sedemikian dinamakan perwakilan digit bertanda.

1.2 Tinjauan

Idea untuk mentransformasikan suatu integer $\bar{n}$ yang berada dalam gelanggang $Z(\tau)$ kepada bentuk kembangan τ-NAF telah dipelopori oleh Solinas (1997). Beliau mengaplikasikannya di dalam algoritma pendaraban skalar $\bar{n}P$ dengan titik asas P melalui lengkuk Koblitz dan telah terbukti bahawa kaedah ini sekurang-kurangnya 50% lebih cepat daripada kaedah kembangan dedua seimbang (rujuk Koblitz (1992)) dan Meier-Staffelbach (rujuk Meier dan Staffelbach (1993)). Ini adalah kerana τ-NAF mampu menghapuskan penggandaan eliptik dan mengekalkan operasi penambahan. Untuk mengekalkan keadaan ini, beberapa kajian telah dilakukan seperti dalam kertaskerja Solinas (1997), Solinas (2000), Joye dan Tymen (2001) dan Hedabou (2006) yang menggantikan τ-NAF dengan suatu kembangan yang berbentuk τ-NAF terturunkan sebagai pengganda pendaraban skalar. Dalam kajian kami, algoritma pendaraban skalar yang kami bangunkan adalah berasaskan kembangan τ-NAF. Kami namakannya sebagai pseudoTNAF. Tinjauan awal ke atas RTNAF yang juga berasaskan kembangan τ-NAF dalam algoritma pendaraban yang telah dibina oleh Solinas (2000), purata bilangan pekali-pekali bukan sifar (iaitu pemberat Hamming) dalam kembangan RTNAF adalah penting untuk menentukan kos pengiraan eliptik. Ini kerana sebahagian kos pengiraan operasi eliptik adalah bergantung kepadanya iaitu setiap pekali bukan sifar akan menggambarkan penambahan kos sebanyak 1. Ini boleh dirujuk di Avanzi et al. (2006). Dengan adanya anggaran kos ini juga, RTNAF mampu menghapuskan penggandaan eliptik dan mengekalkan operasi penambahan. Oleh yang demikian,

analisis semula perlu dibuat ke atas kembangan τ-NAF yang asal bagi mendapatkan formula norma maksimum dan minimum juga purata ketumpatannya (iaitu pemberat Hamming dibahagikan dengan panjang kembangan). Dengan ini kita dapat menganggarkan purata pemberat Hamming bagi pseudoTNAF.

1.3 Pernyataan Masalah

Kajian tentang Kriptografi Lengkuk Eliptik yang kunci rahsia $\bar{n}$nya berasaskan τ-NAF dan mesej asal Pnya di atas lengkuk Koblitz telah berkembang pesat semenjak ianya diperkenalkan oleh Solinas (1997). Sistem yang dapat mengekalkan lebih kurang sama bilangan operasi penambahan eliptik bagi τ-NAF telah dibangunkan oleh Solinas (1997), Solinas (2000), Joye dan Tymen (2001) dan Hedabou (2006) dengan masing-masing menggunakan kembangan τ-NAF kepada $\bar{n} \equiv n \bmod (\tau^m - 1)$, $\bar{n} \equiv n \bmod \frac{\tau^m-1}{\tau-1}$, $\bar{n} \equiv n \bmod \rho(\tau^m - 1)$ dan $\bar{n} \equiv n + r_{hed} \bmod \rho(\tau^m - 1)$. Kajian kami telah mengenalpasti dua kaedah bagaimana untuk mengira kos operasi eliptik. Kaedah pertama sebagaimana yang digunakan oleh Solinas (2000) iaitu dengan mempertimbangkan purata pemberat Hamming bagi kembangan τ-NAF($\bar{n}$). Manakala kaedah yang kedua pula iaitu dengan hanya mempertimbangkan panjang kembangan τ-NAF($\bar{n}$) sepertimana yang dilaksanakan oleh Joye dan Tymen (2001) dan Hedabou (2006).

Kajian kami menjurus kepada pembinaan pendaraban skalar yang kos operasinya setara dengan kaedah yang telah dibangunkan oleh Solinas (1997) dan Solinas (2000) dengan mengunakan kaedah pertama untuk mengira kosnya. Kami akan menggunakan kembangan τ-NAF terturunkan, $\bar{n} \equiv n \bmod \rho\frac{\tau^m-1}{\tau-1}$ (ringkasnya pseudoTNAF($\bar{n}$)). Oleh kerana purata pemberat Hamming bagi pseudoTNAF($\bar{n}$) adalah hasil daripada pendaraban antara purata ketumpatan di kalangan kembangannya yang bersaiz $\bar{l}$ dan panjang maksimumnya apabila $\bar{l} > 30$, maka penganggaran kedua-duanya perlu dilakukan. Kedua-dua anggaran tersebut adalah beracuankan panjang τ-NAF yang asal yang telah diperkenalkan oleh Solinas (1997).

Pertamanya, kami akan menganggarkan panjang maksimum pseudoTNAF($\bar{n}$) yang bersaiz $\bar{l} > 30$ berdasarkan anggaran panjang bagi $\tau-$NAF(n) iaitu

$$log_2 N(n) - 0.54626826939 < l < log_2 N(n) + 3.5155941234 \qquad (1.9)$$

apabila $l > 30$. Batasan panjang bagi $\tau-$NAF(n) ini diperolehi oleh Solinas (2000) dengan mengaplikasikan norma maksimum dan minimum yang terhasil dalam kalangan semua unsur dalam $Z(\tau)$ yang bersaiz $d = 15$ (yakni, $N_{max}(15) = 47324$ dan $N_{min}(15) = 2996$). Beliau menggunakan kaedah penilaian terus yang boleh dirujuk di mukasurat 213 Solinas (2000). Walau bagaimanapun, beliau tidak memberikan perincian kepada kaedah tersebut. Ianya juga terhad kepada d yang bersaiz 1 sehingga 15. Namun demikian, kedua-dua norma tersebut telah dimanfaatkan oleh pengkaji seperti Joye dan Tymen (2001), Hankerson et al. (2004), Avanzi et al. (2006) dan Hedabou (2006) dalam menganggarkan panjang kem-

bangan τ-NAF terturunkan yang bersaiz melebihi 30. Kaedah penilaian langsung boleh diperbaiki dengan memberikan alternatif lain untuk mendapatkan norma maksimum dan minimum yang terjadi dalam kalangan kembangan τ-NAF bagi semua unsur dalam $Z(\tau)$ yang mempunyai sebarang saiz d. Kami menggunakan kaedah transformasi kembangan $\sum_{i=0}^{l-1} c_i\tau^i$ kepada bentuk suatu integer dalam $Z(\tau)$ bagi memperoleh formula normanya. Seterusnya, $N_{max}(d)$ dan $N_{min}(d)$ dengan d suatu integer positif dapat ditentukan. Dengan secara tidak langsung, ini dapat merombak semula pembuktian bahawa anggaran panjang τ-NAF(n) adalah seperti perkaitan (1.9) dengan menggunakan $d = 15$. Oleh yang demikian, panjang maksimum kembangan pseudoTNAF($\bar{n}$) yang bersaiz $\bar{l} > 30$ dapat dijangkakan.

Purata ketumpatan pekali bukan sifar dalam kembangan pseudoTNAF($\bar{n}$) yang bersaiz $\bar{l} > 30$ pula dapat dianggarkan berasaskan purata ketumpatan dalam kalangan τ-NAF yang berasimptot $\frac{1}{3}$ apabila panjang l menghampiri ketakterhinggaan yang diperolehi daripada Solinas (2000). Pembuktian bagi purata ini adalah bertitik-tolak daripada formula purata ketumpatan bagi pekali-pekali bukan sifar dalam kalangan NAF yang mempunyai panjang l. Formula ini diperolehi daripada Morain dan Olivos (1990) seperti berikut:

$$\frac{2^l(3l-4)-(-1)^l(6l-4)}{9(l-1)\left(2^l-(-1)^l\right)}, \tag{1.10}$$

dan juga disebabkan oleh jujukan yang terjadi bagi τ-NAF dengan panjang-l adalah sama sepertimana yang berlaku ke atas NAF dengan panjang-l. Namun demikian, Ratsimihah dan Prodinger (Retrieved 2005) telah menentusahkan bahawa purata ketumpatan pekali-pekali bukan sifar dalam kalangan NAF adalah

$$\frac{1}{3}\left(1+\frac{5}{3l}+\frac{1}{\left(1-(-2)^l\right)}\right). \tag{1.11}$$

Terdapat perbezaan dapatan daripada kedua-dua pengkaji di atas. Oleh itu, analisis semula ke atas τ-NAF yang asal perlu dibuat untuk menentukan salah satu formula, sama ada (1.10) atau (1.11) yang lebih tepat. Formula yang tepat amat diperlukan dalam menentukan purata ketumpatan bagi suatu kembangan pseudoTNAF yang mempunyai panjang tertentu mengikut piawaian antarabangsa seperti dalam NIST (Retrieved July 2013). Penyelidikan ini juga bertujuan untuk menunjukkan bahawa purata ketumpatan τ-NAF adalah berasimptot $\frac{1}{3}$ apabila l menghampiri ketakterhinggaan menggunakan formula yang lebih tepat. Justeru itu, purata ketumpatan pemberat Hamming bagi pseudoTNAF($\bar{n}$) apabila $\bar{l}$ menghampiri ketakterhinggaan dapat dianggarkan. Seterusnya, purata ketumpatan pekali bukan sifar dalam kembangan pseudoTNAF($\bar{n}$) yang bersaiz $\bar{l} > 30$ dapat ditentukan.

1.4 Objektif Kajian

Objektif pertama kajian ini adalah untuk mendapatkan kaedah alternatif kepada kaedah penilaian langsung oleh Solinas (2000) untuk menganggarkan panjang kembangan τ-NAF($\bar{n}$) dengan $l > 30$. Seterusnya, anggaran ini akan digunakan bagi mendapatkan panjang maksimum pseudoTNAF($\bar{n}$). Objektif yang kedua pula adalah untuk membangunkan satu formula yang lebih tepat dari yang digunakan oleh Solinas (2000) untuk membuktikan purata ketumpatan dalam kalangan τ-NAF adalah berasimptot $\frac{1}{3}$ apabila panjang l menghampiri ketakterhingaan. Seterusnya, purata ini akan digunakan untuk menganggarkan purata ketumpatan pseudoTNAF($\bar{n}$) apabila panjang $\bar{l}$ menuju ketakterhingaan. Objektif kajian yang terakhir adalah untuk membina algoritma pendaraban yang hampir setara dari segi kos operasi eliptiknya dengan RTNAF. Ini bertujuan untuk meningkatkan kecekapan pembahagian dalam $Z(\tau)$ tanpa komputasi awal untuk menukarkan $\rho\frac{\tau^m-1}{\tau-1}$ kepada suatu unsur dalam $Z(\tau)$.

1.5 Sumbangan Kajian

Pengkaji selepas ini boleh memanafaatkan formula kembangan τ-NAF berserta normanya untuk mendapatkan norma maksimum dan minimum yang menurut literatur tiada yang seumpamanya sebelum ini. Malah ianya boleh digunakan untuk menganggarkan dengan lebih jitu panjang kembangan τ-NAF bukan hanya setakat $l > 30$ sahaja tetapi $l > 32$ dan yang lebih besar daripada itu. Mereka juga boleh merujuk kaedah yang kami bangunkan untuk membuktikan bahawa purata ketumpatan dalam kalangan τ-NAF adalah berasimptot $\frac{1}{3}$ sebagai alternatif kepada kaedah Solinas (2000). Lebih menguntungkan sekiranya algoritma pendaraban scalar pseudoTNAF daripada kajian ini diaplikasikan ke dalam sistem kriptologi memandangkan kos operasi eliptik yang hampir menyamai RTNAF disamping wujudnya dua kelebihan yang dapat menambahkan kecekapannya. Pertamanya, algoritma penterjemahan $\rho\frac{\tau^m-1}{\tau-1}$ kepada suatu elemen yang berada dalam $Z(\tau)$ dapat mempercepatkan proses pembahagian dalam $Z(\tau)$ untuk sistem kriptografi yang menggunakan nilai $\rho \in Z(\tau)$ khususnya $\rho = 1$ dan $\rho = \tau - 1$. Keduanya, pemilihan kunci rahsia n (iaitu pengganda bagi pendaraban skalar) yang berada di antara julat tertentu dipermudahkan dengan pengaturcaraan bagi mendapatkan purata ketumpatan bagi pekali bukan sifar dalam kembangan pseudoTNAF suatu integer bermodulo $\rho\frac{\tau^m-1}{\tau-1}$ untuk $\rho \in Z(\tau)$. Pengaturcaraan ini menggunakan perisian Maple 13. Ianya juga boleh diadaptasikan khususnya untuk nilai $\rho = 1$ dan $\rho = \tau - 1$.

1.6 Skop Kajian

Skop kajian kami dibahagikan kepada tiga bahagian: Pertama sekali ialah pembinaan formula baru untuk kembangan τ-NAF dengan memulakan analisis ringkas terhadap bilangan cara menyusun pekali-pekali -1 dan 1 dan surihan t pada panjang kembangan 3 menerusi gambarajah pokok. Norma bagi formula ini digunakan

untuk menentukan norma maksimum dan minimum dalam kalangan τ-NAF yang bersaiz melebihi 30.

Pada bahagian kedua, perbandingan dibuat di antara formula purata pekali-pekali bukan sifar daripada kajian kita dengan yang diperolehi oleh Solinas (2000) dan kajian yang dihasilkan oleh Ratsimihah dan Prodinger (Retrieved 2005) dengan analisisnya terhadap NAF. Seterusnya analisis dibuat untuk menentukan yang mana lebih tepat dalam kalangan formula-formula tersebut. Purata ketumpatan dalam kalangan τ-NAF kemudiannya akan dibuktikan berasimptot $\frac{1}{3}$ apabila l menghampiri ketakterhinggaan, sama seperti yang dibuktikan oleh Solinas (2000) dengan menggunakan formula purata pekali-pekali bukan sifar yang lebih tepat.

Pada bahagian terakhir, suatu algoritma pendaraban skalar berasaskan kembangan τ-adic NAF diperkenalkan. Kami namakan teknik tersebut sebagai pseudo τ-adic bukan bersebelahan terturunkan. Kami menggunakan lengkuk Koblitz iaitu sejenis lengkuk khas yang endomorfisma Frobeniusnya boleh digunakan untuk meningkatkan prestasi pengiraan pendaraban skalar. Lengkung Koblitz ini ditakrifkan di atas F_{2^m} seperti Takrifan 1.1. Sifat-sifat lengkuk Koblitz ini dihuraikan lebih lanjut dalam Bab 2.2.4. Pendaraban skalar $\bar{n}P = Q$ dengan P (berperingkat $N\left(\frac{\tau^m-1}{\tau-1}\right)$ suatu perdana) dan Q yang melalui lengkuk tersebut diungkapkan dalam bentuk asas polinomial. Pendaraban titik-titik di atas lengkuk Koblitz adalah bersandarkan operasi penambahan dan penggandaan dalam lengkuk eliptik bukan supersingular. Kami memilih pengganda pendaraban skalar, $\bar{n} \equiv n \bmod \rho\frac{\tau^{m-1}}{\tau-1}$ dengan $\rho \in Z(\tau)$, $n \in Z^+$, nombor perdana $m > 2$ dan pemetaan Frobenius τ seperti dalam Takrif 1.2. Sifat persilangan antara $(r + s\tau)Z(\tau)$ dan Z diperhalusi bagi memilih integer n yang sesuai yang berada di dalam $\left[1, N\left(\frac{\tau^m-1}{\tau-1}\right) - 1\right]$. Dalam algoritma tersebut, kami mengimplimentasikan algoritma untuk pembahagian dalam $Z(\tau)$ yang dibangunkan oleh Solinas (1997) dan mengimplimentasikan algoritma untuk menukarkan suatu bentuk integer dalam $Z(\tau)$ kepada kembangan τ-adic juga oleh Solinas (2000). Untuk mempercepatkan proses pendaraban antara unsur $\rho \in Z(\tau)$ dengan $\frac{\tau^m-1}{\tau-1}$, suatu algoritma penterjemahan/ pendarabannya dibina berasaskan jujukan Lucas. Anggaran kos operasi eliptik akan diteliti dengan merujuk kepada purata pemberat Hamming pseudoTNAF($\bar{n}$) yang bersaiz $\bar{l} > 30$. Ini akan dijadikan kayu pengukur untuk menentukan adakah algoritma pendaraban yang dibina lebih berkesan berbanding RTNAF.

1.7 Penstrukturan Thesis

Tesis ini distrukturkan seperti berikut:
Dalam Bab 2, kami memberikan latarbelakang matematik yang akan digunakan dalam kajian ini. Manakala bahagian ke dua meliputi tinjauan literatur yang berkaitan dengan kajian ini.

Dalam Bab 3, kami memberikan formula baru bagi kembangan τ-NAF(n) untuk setiap panjang l. Seterusnya dapatan ini digunakan untuk menilai norma maksimum dan minimum yang terjadi dalam kalangan semua unsur dalam $Z(\tau)$ yang mempunyai panjang-l. Dalam bab ini juga dibincangkan kaedah bagaimana purata pemberat Hamming bagi kembangan τ-adic diperolehi. Ini merupakan elemen penting untuk membuktikan bahawa purata ketumpatan dalam kalangan τ-NAF berasimptot $\frac{1}{3}$.

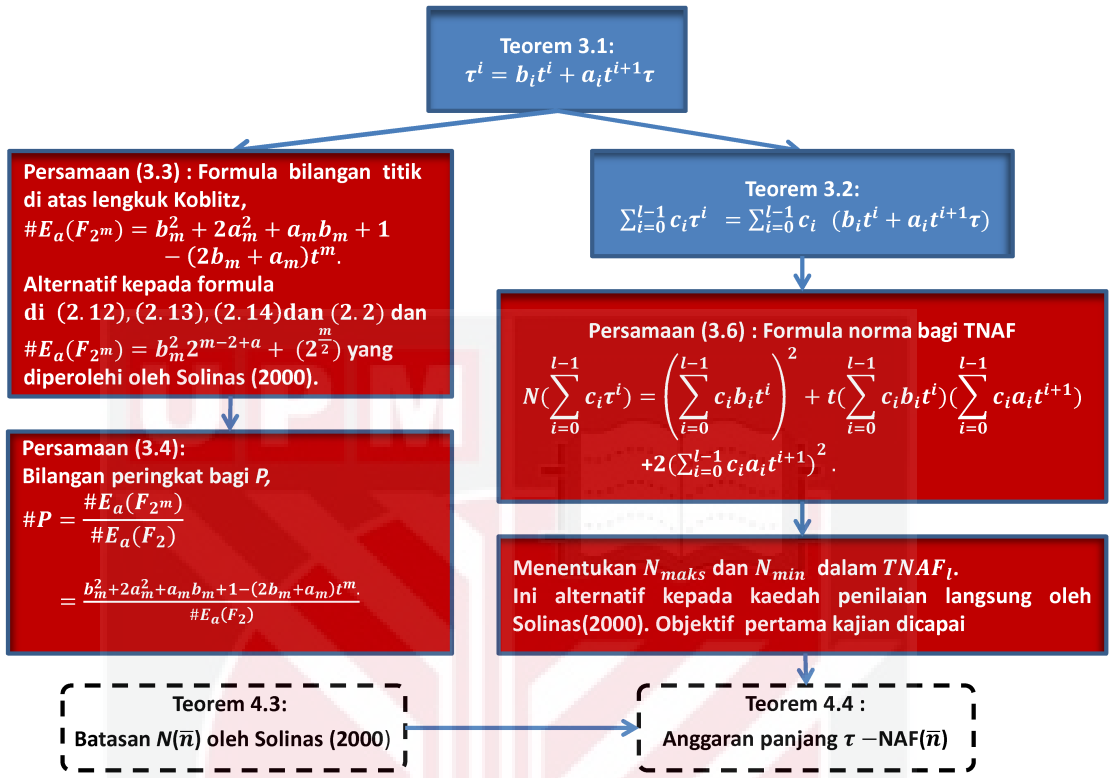
Bab 4, kami mengemukakan bukti bahawa ungkapan berbentuk pseudoTNAF adalah setara dengan τ-NAF yang asal. Kami turut mengemukakan algoritma untuk mendarabkan $\rho \in Z(\tau)$ dengan $\frac{\tau^m-1}{\tau-1}$. Selain daripada itu, diperkenalkan satu algoritma untuk mencari semua titik dalam mod $r + s\tau$ dengan r dan s sebarang integer berpandukan formula jumlah titik kekisi berbeza dalam rantau Voronoi $\rho\frac{\tau^m-1}{\tau-1}Z(\tau)$. Di akhir bab ini, purata pemberat Hamming bagi kembangan pseudoTNAF yang mempunyai panjang maksimum dianggarkan.

Bab 5, kami membangunkan algoritma pendaraban skalar bagi lengkuk Koblitz analog kepada τ-NAF seterusnya membincangkan tentang anggaran kos operasi eliptik algoritma ini yang mempengaruhi keberkesannannya dalam pendaraban skalar.

Bab terakhir merupakan kesimpulan dan cadangan kajian akan datang.

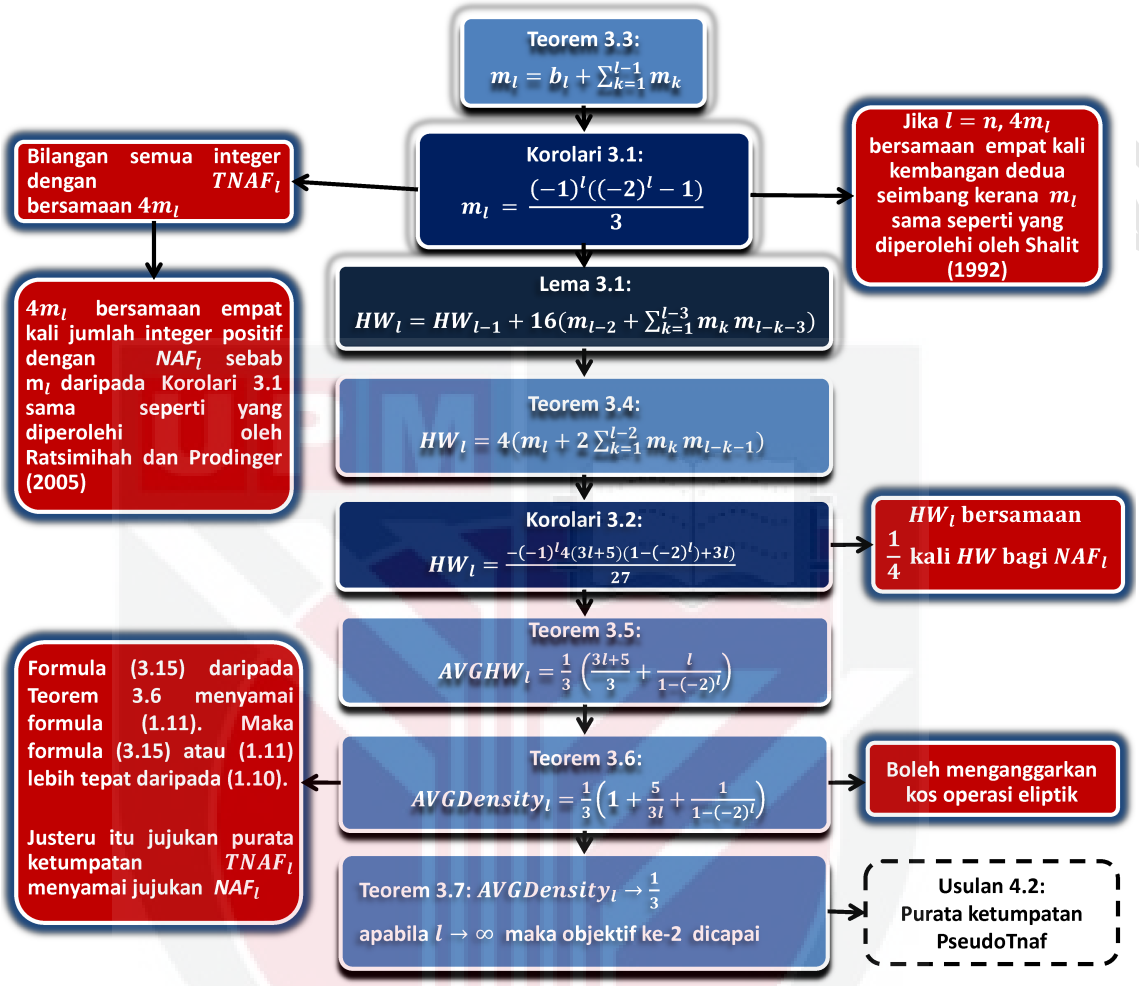
1.8 Carta Alir Penyelidikan

Rajah 1.1 merupakan carta alir menunjukkan bagaimana objektif pertama kajian ini dicapai bermula daripada Teorem 3.1.



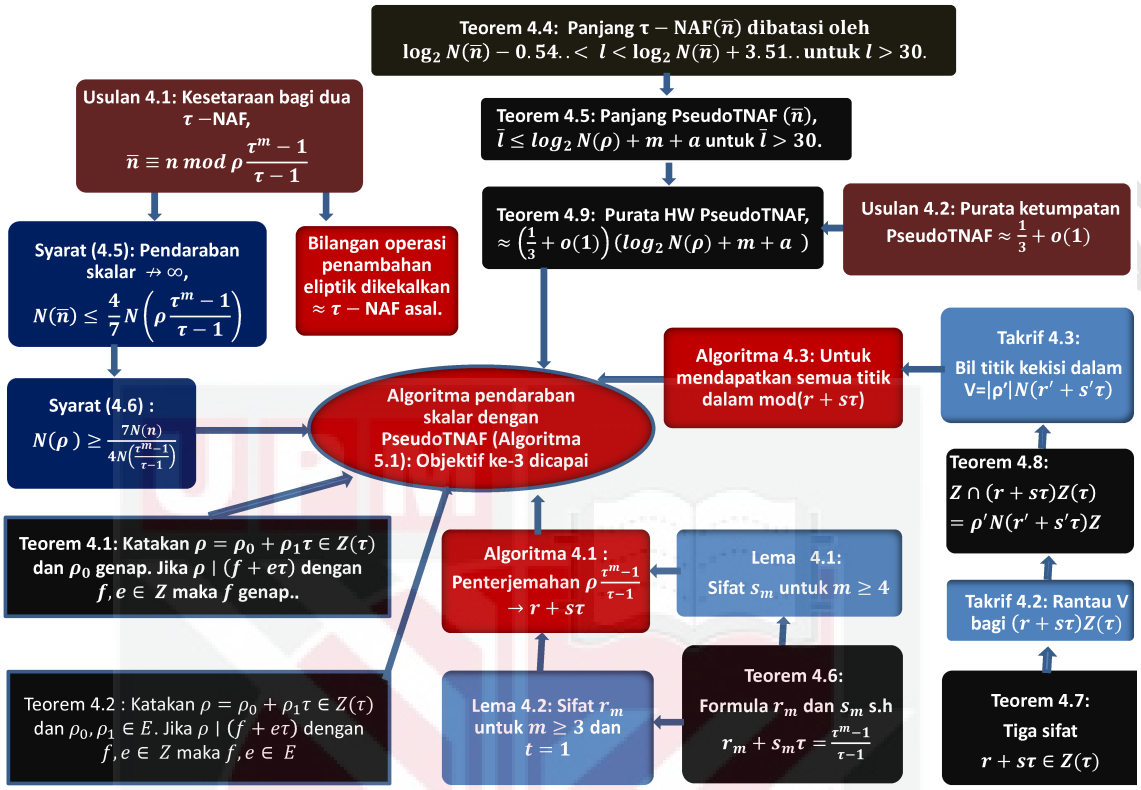
Rajah 1.1: Hasil Penyelidikan Berkaitan τ−NAF

Rajah 1.2 pula merupakan carta alir menunjukkan bagaimana objektif kedua kajian ini dicapai bermula daripada Teorem 3.3 sehingga Teorem 3.7.



Rajah 1.2: Hasil Penyelidikan Berkaitan τ−NAF (Sambungan)

Proses bagaimana objektif terakhir kajian ini dicapai ditunjukkan dalam carta alir Rajah 1.3 yang bermula daripada Teorem 4.4.



1

Rajah 1.3: Hasil Penyelidikan Berkaitan PseudoTNAF

RUJUKAN

Ash, D. W., Blake, I. F. dan Vanstone, S. A. 1989. Low Complexity Normal Bases. *Discrete Applied Math.* 25: 191–210.

Avanzi, R., Heuberger, C. dan Prodinger, H. 2006. Scalar Multiplication on Koblitz Curves. Using the Frobenius Endomorphism and its Combination with Point Halving. *Extensions and Mathematical Analysis, Algorithmica* 46: 249–270.

Avanzi, R. dan Sica, F. Retrieved 2006, Website, https://eprint.iacr.org/2006/067.pdf.

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

Avanzi, R. M., Heuberger, C. dan Prodinger, H. 2011. Redundant τ-adic Expansions I: Non- Adjacent Digit Sets and their Applications to Scalar Multiplication. *Des. Codes Cryptography* 58 (2): 173–202.

Avanzi, R. M., Heuberger, C. dan Prodinger, H. Retrieved 11/08/2010, Website, http://eprint.iacr.org/2010/436.

Avanzi, R. M., Heuberger, C. dan Prodinger, H. Retrieved 2005, Website, http://eprint.iacr.org/2005/225.pdf.

Blake, I. F., Murty, V. K. dan Xu, G. 2008. Nonadjacent Radix-τ Expansions of Integers in Euclidean Imaginary Quadratic Number Fields. *Canadian Journal of Mathematics* 60 (6): 1267–1282.

Booth, A. D. 1951. A Signed Binary Multiplication Technique. *The Quarterly Journal of Mechanics and Applied Mathematics* 4 (2): 236–240.

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

Certicom. Retrieved 1998, Website, http://www.certicom.com.

Cheon, J. H. dan Lee, D. H. 2006. Use of Sparse and/or Complex Exponents in Batch Verification of Exponentiations. *IEEE Transactions on Computers* 55 (12): 1536–1542.

Cheon, J. H. dan Yi, J. H. 2007. Fast Batch Verification of Multiple Signatures. In *Proceeding of the 10th International Conference on Practice and Theory in Public Key Cryptography, PKC 2007*, 442–457. New York: Springer-Verlag.

Coron, J. S. 1999. Resistence against Differential Power Analysis for ECC. In *Cryptographic Hardware and Embeddded Systems (CHES '99)* (eds. C.Koc dan C.Paar), 292–302. New York: Springer-Verlag.

Gordon, D. M. 1998. A Survey of Fast Exponentiation Methods. *Journal of Algorithms* 27 (AL970913): 129–146.

Hakuta, K., Katoh, Y., Sato, H. dan Takagi, T. 2013. Batch Verification Suitable for Efficiently Verifying a Limited Number of Signatures. In *Proceeding of the 15th International Conference on Information Security and Cryptology, ICISC 2012*, 425–440. Springer-Verlag.

Hakuta, K., Sato, H. dan Takagi, T. 2010a. Efficient Arithmetic on Subfield Elliptic Curves over Small Finite Fields of Odd Characteristic. *Journal of Mathematical Cryptology* 4 (3): 199–238.

Hakuta, K., Sato, H. dan Takagi, T. Retrieved 08/02/2014, Website, http://arxiv-web3.library.cornell.edu/abs/1402.1865?context=math.

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

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

Hedabou, M. 2006. A Frobenius Map Approach for An Efficient and Secure Multiplication on Koblitz Curves. *International Journal Of Network Security* 3 (3): 233–237.

Heuberger, C. 2010. Redundant τ-adic Expansions II: Non-Optimality and Chaotic Behaviour. *Mathematics in Computer Science* 3 (2): 141–157.

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

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

Heuberger, C. dan Krenn, D. Retrieved 20/05/2012, Website, http://arxiv.org/pdf/1205.4414v1.pdf.

Joye, M. 2003. Elliptic Curves and Side-Channel Analysis. *ST Journal of System Research* 4(1): 283–306.

Joye, M. dan Tymen, C. 2001. Protection against Differential Analysis for Elliptic Curve Cryptography:An Algebraic Approach. In *Cryptography Hardware and Embedded Systems-CHES01*, 377–390. New York: Springer-Verlag.

Knuth, D. E. 1986. *The Art of Computer Programming*. 3rd edn., *Computer Science and Information Processing*, vol. Seminumeral Algorithms. Addison Wesley.

Koblitz, N. 1987. Elliptic Curve Cryptosystem. *Mathematics Computation* 48 (177): 203–209.

Koblitz, N. 1992. CM Curves with Good Cryptographic Properties. In *Proc. Crypto'91*, 279–287. New York: Springer-Verlag.

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

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

Maplesoft. Retrieved 2013, Website, http://www.maplesoft.com/products/system_requirements.aspx.

Meier, W. dan Staffelbach, O. 1993. Efficient Multiplication on Certain Nonsupersingular Elliptic Curves. In *Proc. Crypto '92*, 333–344. New York: Springer-Verlag.

Miller, V. S. 1986. Use of Elliptic Curve in Cryptography. In *Advance in Cryptology, CRYPTO '85* (ed. H. Williams), 417–426. Springer-Verlag.

Morain, F. dan Olivos, J. 1990. Speeding up the Computations on an Elliptic Curve using Addition-substraction Chains. *Inform Theory. Appl* 24: 531–543.

Muller, V. 1998. Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two. *Journal of Cryptology* 11: 219–234.

NIST. Retrieved July 2013, Website, http://nvlpubs.nist.gov/nistpubs/FIPS/-NIST.FIPS.186-4.pdf.

Ratsimihah, J. R. dan Prodinger, H. Retrieved 2005, Website, http://resources.aims.ac.za/archive/2005/joel.ps.

Reitwiesner, G. W. 1960. Binary Arithmetic. *Advances in Computers* 1: 231–308.

Roy, S. S., Robeiro, C., Mukhopadhyay, D., Takahashi, J. dan Fukunaga, T. Retrieved 2011, Website, http://eprint.iacr.org/2011/318.pdf.

Shallit, J. Retrieved July 1992, Website, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.93.5250.

Solinas, J. A. 1997. An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. In *Advance in Cryptology-CRYPTO '97* (ed. B.Kaliski), 357–371. New York: Springer-Verlag.

Solinas, J. A. 2000. Efficient Arithmetic on Koblitz Curves. *Design, Codes, and Cryptography* 19: 195–249.

Wikipedia. Retrieved 05/05/2014, Website, http://en.wikipedia.org/wiki/Non-adjacent_form.

Wikipedia. Retrieved December 2009, Website, http://en.wikipedia.org/wiki/Signed-digit_representation.

Wikipedia. Retrieved January 2013, Website, http://en.wikipedia.org/wiki/MIPS-year.

Wikipedia. Retrieved March 2013, Website, http://en.wikipedia.org/wiki/Booth's-_mul-tiplication_algorithm.

BIODATA PELAJAR

Faridah Binti Yunos telah dilahirkan di Benut, Pontian, Johor pada 13 Jun 1972. Beliau mendapat pendidikan rendah di Sekolah Rendah Kebangsaan Benut. Pendidikan menengah bermula pada tahun 1985 dengan memasuki Sekolah Menengah Rendah Benut dan kemudian pada tahun 1987, beliau menyambung pelajaran di Sekolah Menengah Benut sehingga Tingkatan 5. Pada tahun 1990, beliau melanjutkan pengajian di Universiti Pertanian Malaysia (UPM), Serdang, Selangor dengan mengambil jurusan Matrikulasi Sains Hayat dan seterusnya pada tahun 1992 ditawarkan mengikuti kursus Bacelor Sains (Kepujian) di dalam bidang Matematik dengan minor komputer di universiti yang sama. Beliau telah dianugerahkan Ijazah Sarjana Muda Matematik pada bulan Julai 1996.

Pada Mei 1996, beliau telah memulakan tugas sebagai Guru Sains (Matematik) di Pusat Pengajian Matrikulasi, UPM sehinggalah April 2000. Beliau seterusnya menyambung tugas di Jabatan Matematik, Fakulti Sains dan Pengajian Alam Sekitar, UPM sebagai Tutor sehingga Jun 2001. Ketika bertugas sebagai Guru Sains dan Tutor, beliau turut mengikuti pengajian dalam program Master Sains di universiti yang sama dan bergraduat pada tahun 2001 dengan memperolehi Master Sains dalam bidang Teori Nombor. Beliau kini adalah pensyarah di Jabatan Matematik, Fakulti Sains, Universiti Putra Malaysia.

SENARAI PENERBITAN

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

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

3. **Yunos, F.**, Mohd Atan, K.A., Md Said, M.R. and Kamel Ariffin, M.R. 2014. Pseudo $\tau-$adic Non Adjacent Form for Scalar Multiplication on Koblitz Curves. *In Proceedings of the 4th International Cryptology and Information Security Conference 2014*, 120-130. Institute of Mathematical Research, Universiti Putra Malaysia.

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : SEM 2 2014/2015

TITLE OF THESIS / PROJECT REPORT :

KEMBANGAN PSEUDOTNAF UNTUK PENDARABAN SKALAR DI ATAS LENGKUK KOBLITZ

NAME OF STUDENT : FARIDAH BINTI YUNOS

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as :

*Please tick (√)

☐	**CONFIDENTIAL**	(Contain confidential information under Official Secret Act 1972).
☐	**RESTRICTED**	(Contains restricted information as specified by the organization/institution where research was done).
☑	**OPEN ACCESS**	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for :

☐ **PATENT** Embargo from _____ (date) until _____ (date)

Approved by:

(Signature of Student)
New IC No/ Passport No.: 720613-01-5770
Date :

(Signature of Chairman of Supervisory Committee)
Name: PROF. DATO' DR. KAMEL ARIFFIN BIN MOHD ATAN, Ph.D.
Date :

[Note : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]