THE FOURTH ORDER LINEAR RECURRENCE SEQUENCE FOR RSA-TYPE CRYPTOSYSTEM

By

WONG TZE JIN

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

February 2006

DEDICATION

To my God Jehovah

for his grace, kindness and love.

All glories, praises and thanksgivings

to Him in the highest.

Scripture

Psalm 111:10
"The fear of Jehovah is the beginning of wisdom; a good understanding have all they that do his commandments: His praise endureth for ever."

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

THE FOURTH ORDER LINEAR RECURRENCE SEQUENCE FOR RSA-TYPE CRYPTOSYSTEM

By

WONG TZE JIN

February 2006

Chairman: Associate Professor Mohamad Rushdan Mohd. Said, PhD

Institute: Mathematical Research

A cryptosystem is derived from the fourth order linear recurrence relations analogous to the RSA cryptosystem which is based on Lucas sequences. The fourth order linear recurrence sequence is a sequence of integers $V_n = PV_{n-1} - QV_{n-2} + RV_{n-3} - SV_{n-4}$, where P, Q, R and S are coefficients in quartic polynomial, $x^4 - Px^3 + Qx^2 - Rx + S = 0$.

The factorization of the quartic polynomial modulo p can be classified into five major types. We define the cyclic structure for every types. Then, we can generate the Euler totient function from the cyclic structure of every types of the quartic polynomial.

We have some properties of the sequence which are straightforward consequences of the definition. Then, we are able to define the composition and inverse of fourth order linear recurrence sequence.

From cycles and totient, we know the quartic polynomial can be factorized into five major types, that is $t[4]$, $t[3,1]$, $t[2,1]$, $t[2]$ and $t[1]$. We sketch an algorithm to compute the type of a quartic polynomial in $\mathbf{F}_p[x]$, where p is any prime number.

In this quartic cryptosystem, we have two large secret primes p and q, the product N of which is part of the encryption key. The encryption key is (e, N) where e is relatively prime to $\Phi(N)$, which are analogous to Euler-ϕ function, to cover all possible cases. The decoding key, d is inverse e modulo $\Phi(N)$.

For quartic cryptosystem, (P,Q,R) constitutes the message, and (C_1, C_2, C_3) constitutes the ciphertext. In decoding, we are given the function $g(x) = x^4 - C_1x^3 + C_2x^2 - C_3x + 1$ but not $f(x) = x^4 - Px^3 + Qx^2 - Rx + 1$, and so we have to deduce the type of f in order to apply the algorithm correctly.

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

JUJUKAN JADI SEMULA LINEAR PERINGKAT KE-EMPAT BAGI SISTEM KRIPTO JENIS RSA

By

WONG TZE JIN

Februari 2006

Pengerusi: Profesor Madya Mohamad Rushdan Mohamad Said, PhD

Institut: Penyelidikan Matematik

Satu sistem kripto diterbit daripada jujukan jadi semula linear peringkat keempat yang sama seperti sistem kripto RSA, berdasarkan dari jujukan Lucas. Jujukan jadi semula linear peringkat keempat adalah satu jujukan interger $V_n = PV_{n-1} - QV_{n-2} + RV_{n-3} - SV_{n-4}$, di mana P, Q, R dan S adalah pekali bagi polinomial kuartik $x^4 - Px^3 + Qx^2 - Rx + S = 0$.

Pemfaktoran bagi polinomial kuartik modulo p dapat dikelaskan kepada lima jenis utama. Kita taktifkan struktur kitaran bagi setiap jenis. Kemudian, kita boleh jana fungsi Euler totient daripada struktur kitaran bagi setiap jenis polinomial kuartik.

Sifat-sifat bagi jujukan Lucas dapat diperolehi daripada takrifan. Kemudian, kita dapat taktifkan penggubahan and funsi songsangan bagi jujukan jadi semula linear peringkat ke-empat.

Daripada kitaran dan totient, kita tahu polinomial kuartik dapat difaktorkan kepada lima jenis utama, iaitu *t*[4], *t*[3,1], *t*[2,1], *t*[2] dan *t*[1]. Kita lakarkan satu algoritma untuk mengira jenis kuartik polinomial dalam $\mathbf{F}_p[x]$, di mana *p* adalah sebarang nombor perdana.

Di dalam sistem kripto kuartik ini, *N* adalah hasil darab daripada dua nombor perdana yang besar *p* dan *q* yang juga merupakan sebahagian daripada kunci enkripsi. Kunci enkripsi ialah (*e*, *N*) di mana *e* secara relative perdana kepada $\Phi(N)$ dan ini adalah sama seperti fungsi Euler-ϕ yang meliputi semua kes-kes kemungkinan. Kunci menyahkod, *d* adalah songsangan bagi *e* modulo $\Phi(N)$.

Bagi sistem kripto kuartik, (*P,Q,R*) adalah mesej dan (C_1, C_2, C_3) adalah teks sifer. Dalam menyahkod, kita diberikan fungsi $g(x) = x^4 - C_1x^3 + C_2x^2 - C_3x + 1$ tetapi tidak $f(x) = x^4 - Px^3 + Qx^2 - Rx + 1$. Oleh itu, kita perlu buat kesimpulan tentang jenis *f* sebelum dapat menggunakan algoritma dengan betul.

ACKNOWLEDGEMENTS

I would like to acknowledge those who assisted me directly or indirectly in the completion of this thesis. Firstly, I am very much indebted to my Lord, Jesus Christ for his blessing.

Secondly, I would like to thank my supervisor, Assoc. Prof. Dr. Mohamad Rushdan bin Md Said and Co-supervisor, Prof. Dato' Dr. Kamel Ariffin bin Mohamad Atan and Assoc. Prof. Dr. Bekbaev Ural for their guidance, patience and support in my research. Their extensive knowledge has contributed a lot in preparing, researching and writing up this thesis.

I would like to express my gratitude to Institute for Mathematical Research, University of Putra Malaysia. Also, my appreciation goes to my friends who encouraged me during the preparation of this thesis.

Lastly, I would like to thank my family; especially my parents for their support and understanding during the course of my studies.

I certify that an Examination Committee has met on 16th February 2006 to conduct the final examination of Wong Tze Jin on his Master of Science thesis entitled "The Fourth Order Linear Recurrence Sequence for RSA-Type Cryptosystem" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

Peng Yee Hock, PhD
Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohamed Othman, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Adem Kilicman, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Zailani Mohamed Sidek, PhD
Associate Professor
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia
(External Examiner)

_____
HASANAH MOHD. GHAZALI, PhD
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date :

This thesis 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 are as follows:

Mohamad Rushdan Mohd. Said, PhD
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Chairman)

Dato' Kamel Ariffin Mohd. Atan, PhD
Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

Bekbaev Ural, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

_____
AINI IDERIS, PhD
Professor/Dean
School of Graduate Studies
Universiti Putra Malaysia

Date :

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

WONG TZE JIN

Date :

TABLE OF CONTENTS