A RSA-TYPE CRYPTOSYSTEM BASED ON QUARTIC POLYNOMIALS

WONG TZE JIN

IPM 2011 19

A RSA-TYPE CRYPTOSYSTEM BASED ON QUARTIC POLYNOMIALS

By

WONG TZE JIN

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

April 2011

DEDICATION

I dedicate this thesis to my Love. Without her, the completion of this work would not been possible.

Scripture

Ephesians*5:25*
"Husbands, love your wives, even as Christ also loved the church, and gave himself for it."

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

A RSA-TYPE CRYPTOSYSTEM BASED ON QUARTIC POLYNOMIALS

By

WONG TZE JIN

April 2011

Chairman: **Associate Professor Mohamad Rushdan Mohd. Said, PhD**

Institute: **Mathematical Research**

RSA cryptosystem was introduced by Rivest, Shamir, and Adleman in 1978. Common users of RSA cryptosystem are currently using 1024-bit keys. They are recommended to use 2048-bit keys in 2011 and 3072-bit key in 2031. However, increasing the bit of keys will decrease the efficiency and increase the cost. Therefore, the aim of this study is to analyze and implement a new cryptosystem which is more secure than RSA, LUC and LUC_3 cryptosystem for same bit of keys. This cryptosystem which is called $LUC_{4,6}$ cryptosystem is derived from a fourth and sixth order Lucas sequence and is based on quartic polynomial.

In this research, numerous mathematical attacks will be analyzed with the cryptosystem and compared with RSA, LUC, and LUC_3 cryptosystems. The numerous mathematical attacks are Hastad's attack, GCD attack, garbage-man-in-the-middle (I) attack, chosen plaintext attack, garbage-man-in-the-middle (II) attack, common modulus attack, Wiener's attack, Lentra's attack and faults based attack.

Most of these attacks have shown that the $LUC_{4,6}$ cryptosystem is secure than RSA, LUC, and LUC_3 cryptosystems. The other attacks have shown that they are in the same security level. This is because these attacks do not result from a weakness of cryptosystem but rather from a bad implementation.

The efficiency of the cryptosystem is the ability to compute e-th term of the fourth and sixth order of Lucas sequence in a reasonable period of time. Therefore, instate of computing V_e sequentially, a new algorithm will be presented to compute V_e in less away of time by omitting some terms in the calculations. By using this algorithm, the time for computations will be decreased. As a conclusion, this cryptosystem has the potential to replace the RSA cryptosystem in the future.

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

SISTEM KRIPTO JESIS RSA BERDASARKAN KEPADA POLINOMIAL KUARTIK

Oleh

WONG TZE JIN

April 2011

Pengerusi: Profesor Madya Mohamad Rushdan Mohamad Said, PhD

Institut: PenyelidikanMatematik

Sistem kripto RSA diperkenalkan oleh Rivest, Shamir, dan Adleman pada tahun 1978. Kini, pengguna umum bagi sistem kripto RSA menggunakan 1024-bit kunci. Mereka disaran menggunakan 2048-bit kekunci pada tahun 2011 dan 3072-bit kekunci pada tahun 2031. Penambahan kekunci bit akan mengurangkan kecekapan dan menambah perbelanjaan. Oleh itu, tujuan kajian ini adalah menganalisa dan melaksanakan suatu sistem kripto yang lebih selamat daripada sistem kripto RSA, LUC dan LUC_3 bagi kekunci bit yang sama. Sistem kripto ini dipanggil sebagai system kripto $LUC_{4,6}$. Sistem ini diterbitkan daripada peringkat ke-empat dan ke-enam jujukan Lucas dan ianya berdasarkan kepada polinomial kuartik.

Dalam penyelidikan ini, banyak serangan matematik akan dianalisa terhadap sistem kripto ini dan ianya dibanding dengan sistem kripto RSA, LUC dan LUC_3. Serangan-serangan ini ialah serangan Hastad, serangan GCD and serangan "*garbage-man-in-the-middle*" (I), serangan pesan terpilih, serangan "*garbage-man-*

in-the-middle" (II), serangan modulus sepunya, serangan Wiener, serangan Lenstra dan serangan berdasar daripada kesilapan. Kebanyakan serangan menunjukkan bahawa sistem kripto $LUC_{4,6}$ adalah lebih selamat daripada sistem kripto RSA, LUC dan LUC_3. Serangan lain menunjukkan bahawa keselamatan mereka berada pada peringkat yang sama. Ini disebabkan serangan-serangan ini bukan hasil dari kelemahan sistem kripto tetapi lebih dari pelaksanaan yang tidak baik.

Kecekapan bagi sistem kripto $LUC_{4,6}$ adalah kemampuan mengira jangka e bagi jujukan Lucas peringkat ke-empat dan ke-enam dalam jangka masa yang munasabah. Oleh itu, selain dari mengira V_e secara jujukan biasa, suatu algoritma baru akan dibentang untuk mengira V_e dalam masa yang lebih pendek dengan mengabaikan beberapa sebutan dalam pengiraan. Dengan menggunakan algoritma ini, jangka masa untuk pengiraan akan dikurangkan. Sebagai kesimpulan, sistem kripto ini mempunyai kesanggupan mengganti sistem kripto RSA pada masa depan.

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 supervisory committee, Assoc. Prof. Dr. Mohamad Rushdan bin Md Said, Prof. Dr. Mohamed bin Othman and Prof. Dato' Dr. Hj. Kamel Ariffin bin Mohamad Atan for their guidance, patience and support in my research. Their extensive knowledge has contributed a lot in preparing, researching and writing up this thesis.

Thirdly, I would like to thank National Science Fellowship, Ministry of Science, Technology and Innovation for their financial support.

Fourthly, I would like to express my gratitude to Institute for Mathematical Research, Universiti 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.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATION

Abbreviation	Description
mod	Modulus
gcd	Greatest common divisor
lcm	Least common multiple
$\emptyset$ or Φ	Euler totient function
V_k	k-th term of Lucas sequence
$U_k{}'$	k-th term of second type of Lucas sequence
$U_k{}''$	k-th term of third type of Lucas sequence
$U_k{}'''$	k-th term of fourth type of Lucas sequence
$U_k{}^{IV}$	k-th term of fifth type of Lucas sequence
$U_k{}^{V}$	k-th term of sixth type of Lucas sequence
D_k	k-th term of Dickson polynomial
T_k	k-th term of a linear recurrence
$P, Q, R,$ and S	Coefficients of Quartic Polynomial
$\beta_1,\ \beta_2,\ \beta_3,$ and β_4	Roots of Quartic Polynomial
$b_1, b_2, b_3, b_4, b_5,$ and b_6	Coefficients of Sextic Polynomial
$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5,$ and α_6	Roots of Sextic Polynomial
ω	cube root of unity, $\omega = \frac{1}{2}\left(-1 + \sqrt[2]{-3}\right)$
$f(x)$ or f or $g(x)$ or g	Function of x
$X_i(x_1, x_2, x_3)$ or $Y_i(x_1, x_2, x_3)$	Function with three variables x_1, x_2, x_3
D	Discriminant of polynomial
$t[k]$	Type of polynomial

$f[t[k]]$ or $g[t[k]]$	Function of type $t[k]$
Z	Set of integer numbers
Z_p	Set of integer numbers over p
$\mathbf{F}_p$	Finite flied over p
$\left(\frac{a}{p}\right)$	Legendre Symbol
e or e_i	Encryption key
d or d_i	Decryption key
$\hat{d}$	Corrupt decryption key
n or n_i	RSA-modulus
$E(x_i)$	Encryption Process
$D(x_i)$	Decryption Process
$R(x_i)$	Recovering Process
m_i	Plaintext
c_i	Ciphertext
s_i	Signature
m_i'	Secondary plaintext
c_i'	Secondary ciphertext
s_i'	Secondary signature
$\hat{s}_i$	Faulty signature

CHAPTER 1

INTRODUCTION

1.1 Overview

In this research, a public key cryptosystem which was derived from the fourth order linear recurrence relation is presented. It is called "The fourth and sixth order of LUC cryptosystem" or "$LUC_{4,6}$ cryptosystem". This cryptosystem is analogous to the RSA, LUC and LUC_3 cryptosystems and based on the Lucas function.

From the Lucas function relationship of this cryptosystem, it is necessary to use the fourth and sixth order of the Lucas sequence to develop the processes of encryption and decryption. Like the RSA cryptosystem, the Euler totient function will assist in determining the decryption key. Besides that, it is necessary to determine the type of quartic equation in which the coefficients are the plaintexts.

The security aspect is the crucial part in the cryptosystem. There are numerous mathematical attacks on RSA-type cryptosystem. Basically, it can be separated into three categories, which are polynomial attacks, homomorphic attacks and other attacks. The polynomial attacks exploits the polynomial structure of RSA. The homomorphic attacks are based on the homomorphic nature. The other attacks like Wiener's attack, Lenstra's attack, and fault based attack do not really result from a weakness of RSA but rather from a bad implementation.

1.2 Problem Statements

The security and efficiency aspects are crucial parts for any cryptosystem. Insecure or inefficient cryptosystem will eventually fall into disuse. Common users of RSA cryptosystem are currently using 1024-bit keys. However, in 2003, Shamir and Tromer described "The Weizmann Institute Relation Locator" (TWIRL) which is a hypothetical hardware device designed to speed up the sieving step of the general number field sieve integer factorization algorithm. TWIRL would be able to factor 1024-bit number in a reasonable amount of time and for reasonable costs. Therefore, the users are recommended to use 2048-bit keys and increased to 3072-bit key in 2031. However, the increase of the bit of keys may be beneficial in terms of cost and efficiency. This is because the increase of the bit of keys will incur additional cost and decrease the efficiency. Therefore, it is a good time to develop a new cryptosystem which is more secure than old cryptosystem for same bit of keys.

1.3 Research Objective

The aim of this study is to analyze and implement the security and efficient aspect for a new cryptosystem. For security aspects, a lot of attacks will be looked into the cryptosystem and compared with RSA, LUC, and LUC_3 cryptosystems. For efficiency aspect, a method will be proposed which can enhance the efficiency of the cryptosystem, especially for reduce the time of computations by decrease the length of computations.

1.4 The Contribution of the Research

The research and development of this cryptosystem which is lower in cost and higher in security will benefit especially the banking sector, defence ministries and confidential business systems.

1.5 The Scopes of the Research and Thesis Organization

The scopes of the research are divided into three areas. Firstly, developed a cryptosystem which is used the Lucas sequence and based on quartic polynomial. Because of characteristic for quartic polynomial, fourth and sixth order Lucas sequence will be used to develop the processes encryption and decryption in the cryptosystem. On the other hand, the characteristics for high order Lucas sequence will be identified and used in the attacks. Secondly, the attacks on the $LUC_{4,6}$ cryptosystem will be looked into and compared with RSA, LUC, and LUC_3 cryptosystems. Thirdly, an algorithm will be introduced to decrease the length of computations for the purpose to reduce the computational time.

The thesis organization will be arranged as follows: chapter two contains two parts. The first part is the mathematical background which will be used in this investigation. The second part is reviewing a list of literatures which is related to the study.

Chapter three is the construction of the cryptosystem, which is analogous to the RSA, LUC and LUC_3 cryptosystems. In addition, the extended functions of Lucas sequence will help to solve the homomorphic nature problem for the cryptosystem. Besides that, it will contribute to the proposal of a new method of computations to high order Lucas sequence. The relation between Dickson polynomial and Lucas sequence is the important part in the polynomial structure which can solve the problems in the polynomial attack.

In chapter four, the security aspect is discussed. In this chapter, nine attacks will be analyzed. They are the Hastad's attack, GCD attack, garbage-man-in-the-middle (I) attack, chosen plaintext attack, garbage-man-in-the-middle (II) attack, common modulus attack, Wiener's attack, Lenstra's attack and transient fault based attack.

In chapter five, a method to enhance the computations will be proposed. This method is suitable for high order Lucas sequence.

Chapter six is the conclusion and future research.

REFERENCES

[1] Adams, W. and Shanks, D. 1982. Strong primality tests that are not sufficient. *Mathematics of Computation* 39(159): 255-300.

[2] Bao, F., Deng, R., Han, Y., Jeng, A., Narasimhalu, D., and Ngair T.H. 1997. Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults. *Pre-proceedings of the 1997 Workshop on Security Protocols*, France.

[3] Bleichenbacher D. 1996. *Efficiency and Security of Cryptosystems based on Number Theory*, PhD Thesis, Swiss Federal Institute of Technology Zurich, Zurich.

[4] Bleichenbacher D., Bosma W., and Lenstra A.K. 1995. Some remarks on Lucas-Based Cryptosystems. Lecture Notes in Computer Science 963:386-396.

[5] Bleichenbacher, D., Joye, M., and Quinsquater, J.J. 1997. A New and Optimal Chosen Message attack on RSA-type cryptosystem. *Information and Communications Security, Lecture Notes in Computer Science* 1334: 302-313.

[6] Childs, L.N. 1979. The Discriminant and the Stickelberger's Theorem. In *A Concrete Introduction to Higher Algebra,3rd ed.*, pp 282-289. New York: Springer-Verlag.

[7] Coppersmith, D. 1996. Finding a Small Root of a Univariate Modular Equation. *Lecture Notes in Computer Science* 1070: 155-165.

[8] Diffie, W. and Hellman, M. 1976. New directions in cryptography. *IEEE Transaction on Information Theory* 22: 644-654.

[9] Dickson, L.E. 1897. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *The Annals of Mathematics* 11(1/6): 65–120; 161–183.

[10] Franklin, M.K. and Reiter, M.K. 1995. A linear protocol failure for RSA with exponent three, *Preliminary note for Crypto'95 rump session.*

[11] Hardy G.H. and Wright E.M. 1979. *An Introduction to the Theory of Numbers, 4th ed.*, Oxford: Oxford University press.

[12] Hastad, J. 1986. On using RSA with low exponent in a public key network. *Lecture Notes in Computer Science*218:404-408.

[13] Joye, M. 1996. Common Modulus Attack Against Lucas Based Systems. *Technical ReportCG*-1996/10, UCL Crypto Group, Louvain-la-Neuve.

[14] Joye, M. 1997. *Security Analysis of RSA-type Cryptosystems*. PhD Thesis, Universite Catholique de Louvain, Belgium.

[15] Joye, M. 1997. On the importance of securing your bins: The garbage-man-in-the-middle attack. *Proceeding of the 4th ACM Coference on Computer and Communications Security*, ACM press, pp135-141.

[16] Julta, C.S. 1998. On Finding Small Solutions of Modular Multivariate Polynomial Equations. *Lecture Notes in Computer Science,* 1403:158-170.

[17] Knuth, D.E. 1981. *The Art of Computer Programming,vol.2, Seminumerical Algorithms.* 2nd ed, Massachusetts:Addison-Wesley.

[18] Lidl, R. 1993. Theory and application of Dickson polynomial. *Topics in Polynomials of One and Several Variables and Their Applications*, *World Scientific*, pp371-395.

[19] Montgomery, P.L. 1983. Evaluating Recurrences of Form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas Chains. Unpublished manuscript.

[20] Patarin, J. 1995. Some serious protocol failure for RSA with exponent e of less than $\approx$ 32 bits, Presented at the conference of Cryptography, CIRM Luminy, France.

[21] Pinch, R.G.E. 1995. Extending the Wiener Attack to RSA-type cryptosystems. *Electronics Letters* 31(20): 1736-1738.

[22] Pinch, R.G.E. 1995. Extending The Hastad Attack to LUC. *Electronics Letter*31(21): 1827-1828.

[23] Rivest, R., Shamir, A., and Adleman, L. 1978. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communication of the ACM*21: 120-126.

[24] Said, M.R.M. 1997. *Application of Recurrence Relations to Cryptography.* PhD Thesis, Macquarie University, Australia.

[25] Said, M.R.M and John L. 2003. A Cubic Analogue of the RSA Cryptosystem. *Bulletin of the Australia Mathematical Society* 68: 21-38.

[26] Schneier, B. 1999. Mathematics Background. In *Applied Cryptography, 2nd ed.*, pp 242-254. New York: John Wiley & Son, Inc.

[27] Schroeppel. 1972. Polynomial Discriminant, Mathworld, Wolfram Research, Inc. http://mathworld.wolfram.com/PolynomialDiscriminant.html. Retrieved on 21st May 2009.

[28] Simmons, G.J. 1983. A Weak Privacy Protocol Using the RSA Cryptoalgorithm. *Cryptologia* 7(2): 9-13.

[29] Smith, P.J. and Lennon, M.J.J. 1993. LUC: A New Public Key System. *Proceedings of the Ninth IFIP International Symposium on Computer Security*: 103-117.

[30] Weisstein, E.W. Quartic Equation, Mathworld, Wolfram Web Resource. http://mathworld.wolfram.com/QuarticEquation.html. Retrieved on 21st May 2010.

[31] Weisstein, E.W.Waring Formula, MathWorld, Wolfram Web Resource. http://mathworld.wolfram.com/WaringFormula.html. Retrieved on 21st May 2010.

[32] Weisstein, E.W. Lehmer's Totient Problem. MathWorld, Wolfram Web Resource. http://mathworld.wolfram.com/LehmersTotientProblem.html. Retrieved on 21st May 2010.

[33] Wiener M.J. 1990. Cryptanalysis of Short RSA Secret Exponents. *IEEE Transactions on Information Theory* 36(3): 386-396.

[34] Williams, H.C. 1972. On a Generalization of the Lucas Functions. *Acta Arithmetica* 20: 33-51

[35] Wong, T.J. 2006. *The Fourth Order Linear Recurrence Sequence for RSA-type Cryptosystem*, Master Thesis, Universiti Putra Malaysia, Malaysia.

[36] Yen, S.M. and Laih, C.S. 1995. Fast Algorithms for LUC Digital Signature Computation. *IEEE Proceedings, Computers and Digital Techniques* 142:165-169.