UNIVERSITI PUTRA MALAYSIA

ENHANCING SPEED PERFORMANCE OF THE CRYPTOGRAPHIC ALGORITHM BASED ON THE LUCAS SEQUENCE

ESAM M. ABULKHIRAT

FSKTM 2003 5

ENHANCING SPEED PERFORMANCE OF THE CRYPTOGRAPHIC ALGORITHM BASED ON THE LUCAS SEQUENCE

By

ESAM M. ABULKHIRAT

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

January 2003

Dedicated to my beloved family:

my parents, brothers and sisters

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

ENHANCING SPEED PERFORMANCE OF THE CRYPTOGRAPHIC ALGORITHM BASED ON THE LUCAS SEQUENCE

By

ESAM M. ABULKHIRAT

January 2003

Chairman: Associate Professor Mohamed Othman, Ph.D.

Faculty: Computer Science and Information Technology

Computer information and network security has recently become a popular subject due to the explosive growth of the Internet and the migration of commerce practices to the electronic medium. Thus the authenticity and privacy of the information transmitted and the data stored on networked computers is of utmost importance. The deployment of network security procedures requires the implementation of cryptographic functions. More specifically, these include encryption, decryption, authentication, digital signature algorithms and message-digest functions. Performance has always been the most critical characteristic of a cryptographic function, which determines its effectiveness.

Since the discovery of public-key cryptography, very few convincingly secure asymmetric schemes have been discovered despite considerable research efforts. Utilizing the properties of Lucas functions introduced a public key system based on Lucas functions instead of exponentiation, which offer a good alternative to the most publicly used exponential public key system RSA.

LUC cryptosystem algorithm based on the quadratic and cubic polynomial, is introduced in this thesis with a new formula to distinguishing between the cubic polynomial roots. Reducing the calculation time of the algorithm, in sequential and parallel platforms, using the doubling-rule technique combined with a new scheme led to a strong improvement of the LUC algorithm speed.

The computation time analysis shows that whene doubling with remainder technique is used, the improvement of the speed rises rapidly compared to the standard implementation of the LUC algorithm and LUC algorithm with doubling rule. Furthermore the algorithm is still keeping its simplicity of non-multiplicative and non-exponentiation public-key cryptosystem. The improved algorithm is applied on the lab-PC for the sequential platform, and cluster-computing machine for the parallel platform, which lead to a substantial time reduction and an enhancement of the algorithm speed in both platforms.

Abstrak disertasi yang diserahkan kepada Senat Universiti Putra Malaysia bagi memenuhi keperluan untuk ijazah Master

PEMANTAPAN PRESTASI MASA UNTUK ALGORITMA KRIPTOGRAFI BERDASARKAN JUJUKAN LUCAS

Oleh

ESAM M. ABULKHIRAT

Januari 2003

Pengerusi: Profesor Madya Mohamed Othman, Ph.D.

Fakulti: Sains Komputer dan Teknologi Maklumat

Maklumat komputer dan keselamatan rangkaian komputer telah menjadi subjek popular kerana terdapatnya peningkatan mendadak penggunaan internet dan migrasi aktiviti komersil ke dalam mesin elektronik. Justeru, keautentikan serta kerahsiaan maklumat yang dihantar dan data yang disimpan oleh rangkaian komputer adalah amat penting. Implementasi prosedur keselamatan memerlukan penggunaan fungsi kriptografi secara khusus. Ini merangkumi penyulitan, nyahsulit, pengautentikan, algoritma tandatangan digital dan fungsi 'message-digest'. Prestasi sentiasa menjadi ciri terpenting sesuatu fungsi kriptografi, serta menjadi penentu keberkesanannya.

Sejak penemuan kekunci umum kriptografi, terdapat hanya beberapa penemuan skema berasimetri yang selamat, walaupun banyak usaha penyelidikan yang telah dilakukan. Penggunaan ciri fungsi Lucas telah memperkenalkan sistem kekunci umum berasaskan fungsi tesebut, bukannya berasaskan fungsi bereksponen yang menawarkan alternatif yang baik kepada RSA, sistem kunci umum bereksponen yang paling banyak digunakan.

Dalam tesis ini, algoritma kriptosistem LUC berdasarkan polinomial kuadratik dan kubik diperkenalkan dengan satu formula baru untuk membezakan punca polinomial kubik. Peningkatan prestasi yang ketara telah tercapai dengan mengurangkan masa pengiraan algoritma dalam landasan siri dan selari. Menggunakan kombinasi teknik petua penggandaan dengan teknik baru itu telah menghasilkan peningkatan prestasi yang mendadak dari segi kepantasan algoritma LUC.

Analisis masa pengiraan telah membuktikan bahawa penggunaan teknik baru telah menyebabkan peningkatan prestasi masa, berbanding dengan sistem implementasi piawai, algoritma LUC dan algoritma LUC dengan petua penggandaan. Tambahan pula, algoritma itu masih mengekalkan keringkasan kekunci umum kriptosistem yang tak berdaya darab dan tak bereksponen. Algoritma yang telah ditambah baik ini digunakan pada komputer peribadi (PC), makmal untuk landasan berjujukan dan mesin pengiraan gugusan untuk landasan selari. Ini telah menghasilkan pengurangan masa yang banyak serta pemantapan kepantasan algoritma bagi kedua-dua landasan.

ACKNOWLEDGMENTS

I am very thankful to my supervisor Associate Professor Dr. Mohamed Othman Head Dept. of Communication Technology and Networks, Faculty of Computer Science and Information Technology, for his helpful guidance and suggestions. I also appreciate all the cooperation from the committee members Dr. Mohamad Rushdan Md Said and Dr. Rozita Johari. Thanks to the support that i received from everyone during my research study.

I am very grateful to the Faculty of Computer Science and Information Technology and the staff of Postgraduate office, Library and University Putra Malaysia, for providing a good studying and research environment.

Finally, I would like to thank my parents, my brothers, my sisters, all the family members, and friends for their love, constant support and encouragement in all my endeavors.

ESAM M. ABULKHIRAT

January 2003

This thesis submmitted to the Senate of Universiti Putra Malaysia has been accepted as fulfilment of the requirment for the degree of Master of Science. The members of the Supervisory Committee are as follows:

Ramlan Mahmod, Ph.D.
Associate Professor
Faculty of Computer Science and Information Technology
University Putra Malaysia
(Chairman)

Mohamad Othman, Ph.D.
Associate Professor
Faculty of Science and Environmental Studies
University Putra Malaysia
(Member)

Mohamad Rashdan Md Said, Ph.D.
Faculty of Science and Environmental Studies
University Putra Malaysia
(Member)

Rozita Johari, Ph.D.
Faculty of Computer Science and Information Technology
University Putra Malaysia
(Member)

AINI IDERIS, Ph.D.
Professor/Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

LIST OF ABBREVIATIONS

ATM	Asynchronous Transfer Mode
CPU	Central Processing Unit
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DL	Discrete Logarithm
DoP	Degree of Parallelization
GF	Galois Field
HPF	High Performance Fortran
IFP	Integer Factorization Problem
LAM	Local Area Multicomputers
LAN	Local Area Network
LS	Legendre Symbol
LUC_2	Quadratic Lucas Sequences
LUC_3	Cubic Lucas Sequences
MIMD	Multiple Instructions Multiple Data
MPI	Message Passing Interface
NBS	National Bureau of Standard
NOWs	Network of Workstations
NP	Non Deterministic Polynomial
PINs	Personal Identification Number
PKC	Public Key Cryptography
PVM	Parallel Virtual Machine

RSA	Rivest, Shamir and Adleman
SMP	Symmetric Multiprocessor
SPMD	Single Program Multiple Data

CHAPTER 1

INTRODUCTION

Via the digital world and the cyber space, several limitations of fast communication have been eliminated. Therefore many models and systems are looking for an ideal method to provide a secure environment for better optimization of the electronic-connected world [14]. Cryptography accepts the challenge and play the main role of the modern and secure communication world [10]. Both private [34] and public key [10] techniques were invented in order to secure the data transaction via digital networks.

1.1 Statement of Problem

Modern cryptographic algorithms are used to guarantee that no one but the intended recipient can decipher the contents of the message or the information, based on specific algorithm, which deal with the encryption and decryption operations. Encryption is applied to the message that we intend to send under secure circumstances so it becomes ciphertext. The decryption mechanism converts this ciphertext back to its original form (Plaintext form). Random and big range of bits known as encryption key is used for the encryption and decryption operations [2]. The key size decides the strength of the cryptosystem, at the same time it must satisfy the conditions of the system resources. LUC cryptosystem [41] as an alternative to RSA [31] the most famous Cryptosystem algorithm, is attracted more research concerns, since the big size keys require more computation time and thus keeps the system busy for a long

period of time. Thus the cryptography systems has to integrate security, functionality and performance with the existing system resources [21].

Looking for high performance computing systems to simulate more realistic systems in greater details comes with the parallel computing techniques, which limit the speed of one processor and offer high performance with low cost price [6]. So with the parallelism techniques applied to the cryptographic systems, it points to a bright future of securing and speeding up communications via the networks [25].

1.2 The Research Objectives

This research utilizes the attractive feature of Cryptography without exponentiation, LUC algorithm, the alternative to the most popular cryptography algorithm RSA, and enhance its performance sequentially and parallel. Therefore, the research objectives are:

- To improve the speed performance of the LUC cryptosystem sequentially. Utilizing the available system resources to gain maximum benefits of reducing the consuming time .
- To implement parallelism techniques with the LUC cryptosystem algorithm, in order to improve the performance of LUC algorithm with a multiprocessor machine.

1.3 The Research Scope

Several new techniques and algorithms are used to secure the E-world communication. On the other hand, speeding up their computation and reducing the number of parameters multiplication, are the main cryptography research area that affect the secure communication today. In this thesis, we will concentrate on the Asymmetric (public key) cryptography based on the Lucas sequences, by enhancing the sequential speed of the algorithm, and finding a method of providing more granularity to achieve a parallel computation model. For the parallel model, an explicit parallelism using MPI technique, will be used to distribute and schedule the workload over the processes of multicomputers.

1.4 The Research Importance

Public-key cryptosystem is an essential raw material of the internet. Without public key, the explosive growth of virtual private networks and electronic commerce would be seriously hampered. Encryption is necessary on the internet because of the new dangers that traditional methods of law enforcement do not anticipate. For example, when a computer criminal is wanted for wire fraud, we still put his face on the wall of the Post office. But computer criminals are faceless names on the internet, adept at pretending to be whoever they want. Similarly, the holograms and photo ID techniques used to protect plastic credit cards offer no help when an unadorned credit card number is used to purchase goods or service over the internet. Encryption provides electronic equivalents to many traditional business safeguards. Message au-

thentication programs, for example, do what the unbroken seal on an envelope does- to prove that an e-mail message has not been tampered with. The internet is changing the way we do things. And public-key encryption is an important ingredient in the changing internet. Table 1.1 shows a few of the new ways of doing things that depend at least in part upon a secure internet environment.

Table 1.1 New Ways and Old Ways of Doing Things.

New Ways	Old Ways
Electronic Mail	Letters and Faxes
Virtual Private Networks	Expensive Private Leased Lines
Hypertext Searching	Looking in Indexes of Books
internet Shopping	Catalogs and Crowded Malls
24-hour Online Banking	Waiting in Lines
Express Delivery Tracking	Being on Hold
Digital Signatures	Your Pen-and-Ink John Hancock
Low-cost Stock Trades	Calling Your Broker

Encryption makes words and numbers unreadable. Decryption reverses the process. Encryption is used to keep secrets, ranging from the nation's plans for air defense to your annual salary review. The same technology guards secrets whether they are large or small [42].

Public key technology protects your privacy while allowing you easy and painless access to the information you need. Public key is used specifically for:

Key management . You and I must agree on a key in order to encrypt a message at one end of the transaction and decrypt it at the other. To preserve security, we must change keys frequently. Public key exchange makes key exchange and key management much easier.

User authentication . If you get an e-mail from me, how do you know I really sent it?. Digital signatures are another important part of Public Key technology.

Non-repudiation . Public key digital signatures authorize a merchant to provide the goods or services requested. In case of a dispute, the merchant can produce the signed work order. The internet is already built. Public key technology is like the golden spike that will complete the internet's promise by opening up new applications we can use with confidence.

And since public-key encryption is really mathematics, the encryption key is made out of numbers. It is a string of digits. Key length, therefore refers to the size of the number represented by those digits. The longer the key, the greater the security [14].

Public key technology is based on creating problems that would take all the world's computers working together several dozen lifetimes to solve. Specifically, breaking public-key encryption requires the factorization of very large numbers. As you see, public-key computations require a lot of effort from even the fastest microprocessors. To accomplish variant communication security goals, the cryptography techniques can be installed into different network layers and interfaces such as data link interface, data link layer, device derive interface, and network protocol stack. Moreover, the cryptography techniques are necessary for a wide range of applications such as internet application, wireless communications and telecommunications.

1.5 Thesis Organization

The thesis has seven chapters, including this introductory chapter. As follows:

Chapter 1 Provides the main guide lines of thesis, such as, The problem statement, objectives, scope and the importance of the work.

In Chapter 2 some mathematical background covers the necessary aspects of number theory, related to cryptography and its mathematical architecture.

Chapter 3 contains the literature review that presents two portions of the thesis. The first portion discusses cryptographic algorithms, basic definitions, introduction to public/private keys algorithms, and the most popular public-key cryptography algorithms. The chapter explains the mathematical problems (integer factorization) that has been used in RSA and its extension LUC algorithm.

The second portion discusses Parallel and distributing systems, cluster computing, and message passing models. It also explains the demand for greater computational speed.

Chapter 4 presents quadratic analogue of the RSA cryptosystem. This chapter gives the basic definitions of the LUC_2 cryptography algorithm, the encryption/decryption processes, and the performance of the algorithm.
The key size and the speed of the algorithm are the backbone of this chapter, presenting a new technique of speeding up the algorithm, by using the double step method. It also shows the results of the speed improvement.

Chapter 5 presents cubic analogue of the RSA cryptosystem. In this chapter, we present the basic structure of cubic recurrence sequence, and propose a modified method to distinguish between cubic congruence roots. The chapter ends with LUC_3 encryption/decryption process, and computation efficiency of LUC_3 algorithm.

Chapter 6 contains Parallel implementation of LUC_2 cryptosystem. This chapter discusses and evaluates the parallel code using MPI, and shows the analysis of the results according to the number of used processes and communication/computation time of each number of processes.

Chapter 7 includes the conclusions and recommendation that summarize the most important aspects of the thesis, the significant contributions and ends with future work directions.

CHAPTER 2

MATHEMATICAL BACKGROUND

Computational number theory plays an important role in cryptography because many cryptographic systems and protocols are based on algebraic and number theoretic structures. Among the important number-theoretic problems relevant to cryptography are primality testing, factoring integers, and discrete logarithms in finite groups.

Efficiency and security are two natural but conflicting goals in cryptography. This thesis is concerned with a number of security and efficiency aspects of cryptosystems based on number theory.

There are numerous books devoted to the theory of numbers, good references are [13] and [16]. For the Lucas sequences, we refer to [29] and [30].

2.1 Basic Facts

In this section, we give some well-known results on number theory.
were omitted since they may be found in most textbooks on number theory .