UNIVERSITI PUTRA MALAYSIA

AN IMPROVED PUBLIC KEY CRYPTOGRAPHY BASED ON THE ELLIIPTIC CURVE

ESSAM FALEHAL-DAOUD

FSKTM 2002 2

AN IMPROVED PUBLIC KEY CRYPTOGRAPHY BASED ON THE ELLIPTIC CURVE

ESSAM FALEH AL-DAOUD

DOCTOR OF PHILOSOPHY
UNIVERSITI PUTRA MALAYSIA

2002

AN IMPROVED PUBLIC KEY CRYPTOGRAPHY BASED ON THE ELLIPTIC CURVE

By

ESSAM FALEH AL-DAOUD

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

March 2002

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

AN IMPROVED PUBLIC KEY CRYPTOGRAPHY BASED ON THE ELLIPTIC CURVE

By

ESSAM FALEH AL-DAOUD

March 2002

Chairman: Ramlan Mahmod, Ph.D.

Faculty: Computer Science and Information Technology

Elliptic curve cryptography offers two major benefits over RSA: more security per bit, and a suitable key size for hardware and modern communication. Thus, this results to smaller size of public key certificates, lower power requirements and smaller hardware processors.

Three major approaches are used in this dissertation to enhance the elliptic curve cryptsystems: reducing the number of the elliptic curve group arithmetic operations, speeding up the underlying finite field operations and reducing the size of the transited parameters. A new addition formula in the projective coordinate is introduced, where the analysis for this formula shows that the number of multiplications over the finite field is reduced to nine general field element multiplications. Thus this reduction will speed up the computation of adding two points on the elliptic curve by 11 percent. Moreover, the new formula can be used more efficiently when it is combined with the suggested sparse elements algorithms.

To speed up the underlying finite field operations, several new algorithms are introduced namely: selecting random sparse elements algorithm, finding sparse base points, sparse multiplication over polynomial basis, and sparse multiplication over normal basis. The complexity analysis shows that whenever the sparse techniques are used, the improvement rises to 33 percent compared to the standard projective coordinate formula and improvement of 38 percent compared to affine coordinate. A new algorithm to compress and decompress the sparse elements algorithms are introduced to reduce the size of the transited parameters.

The enhancements are applied on three protocols and two applications. The protocols are Diffie-Hellman, ELGamal and elliptic curve digital signature. In these protocols the speed of encrypting, decrypting and signing the message are increased by 23 to 38 percent. Meanwhile, the size of the public keys are reduced by 37 to 48 percent. The improved algorithms are applied to the on-line and off-line electronic payments systems, which lead to probably the best solution to reduce the objects size and enhance the performance in both systems.

Abstrak dissertasi yang diserahkan ke Senat Universiti Putra Malaysia bagi memenuhi keperluan untuk ijazah Doktor Falsafah

PEMBAIKAN KRIPTOGRAFI KEKUNCI UMUM BERDASARKAN KELUK ELIPTIK

Oleh

ESSAM FALEH AL-DAOUD

Mac 2002

Pengerusi: Ramlan Mahmod, Ph.D.

Fakulti: Sains Komputer dan Teknologi Maklumat

Kriptografi keluk eliptik menawarkan dua kelebihan berbanding RSA: lebih ciri-ciri keselamatan per bit, dan saiz kekunci yang sesuai untuk perkakasan dan komunikasi moden. Ini menghasilkan saiz perakuan kekunci umum lebih kecil, keperluan kuasa yang rendah dan perkakasan pemprosesan yang lebih kecil.

Tiga pendekatan utama digunakan di dalam dissertasi ini untuk meningkatkan sistem kripto keluk eliptik iaitu mengurangkan jumlah operasi arithmetik kumpulan keluk eliptik, mempercepatkan operasi medan terhingga, dan mengurangkan saiz parameter-parameter peralihan. Suatu formula tambahan baru dalam kordinat unjuran diperkenalkan, di mana analisis bagi formula ini menunjukkan jumlah perkalian bagi medan terhingga dikurangkan ke sembilan perkalian elemen medan umum. Maka pengurangannya akan mempercepatkan pengiraan bagi penambahan dua titik diatas keluk eliptik sebanyak 11 peratus. Malah, formula baru ini boleh

digunakan dengan lebih cekap apabila ia digabungkan dengan algoritma elemen-elemen jarang yang dicadangkan.

Bagi mempercepatkan operasi medan terhingga, beberapa algoritma baru diperkenalkan iaitu: algoritma memilih element-elemen jarang secara rawak, mencari titik-titik dasar yang jarang, perkalian jarang ke atas pengkalan normal. Analisis kekompleksan menunjukkan jika sebarang teknik jarang digunakan, peningkatan sebanyak 33 peratus diperolehi berbanding formula kordinat dan 38 peratus jika dibandingkan dengan kordinat affine. Satu algoritma baru untuk memampatkan dan menyahmampat element-elemen jarang diperkenalkan untuk mengurangkan saiz parameter-parameter peralihan.

Peningkatan dilaksanakan ke atas tiga protokol dan dua aplikasi. Protokol-protokol tersebut adalah protokol-protokol Diffie-Hellman, ELGamal dan tanda tangan digital keluk eliptik. Dalam protokol ini, kepantasan untuk mengencrip, nyahsulit dan menanda tangan mesej meningkat sebanyak 23 hingga 38 peratus. Sementara itu saiz kunci umum dikurangkan 37 hingga 48 peratus. Algoritma ini dilaksanakan kepada sistem pembayaran elektronik dalam-talian dan luar-talian. Pendekatan baru ini boleh membawa kepada penghuraian terbaik dengan mengurangkan saiz objek serta meningkatkan presasi kedua-dua sistem.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Associate Professor Dr. Ramlan Mahmod, deputy dean, Faculty of Computer Science and Information Technology, for his helpful supervision, guidance and valuable suggestions. I also thank the committee members Dr. Mohamad Rushdan and Dr. Adem Kilicman for their efforts and valuable comments.

Finally, I am grateful to Faculty of Computer Science and Information Technology, Post Graduate Office and Library, University Putra Malaysia, for providing a good environment for studying and researching.

Essam Al-Daoud

March 2002

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute.
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard.
DHP	Diffie-Hellman Protocol
DLP	Discrete Logarithm Problem
DSA	Digital Signature Algorithm.
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptosystem
ECDL	Elliptic Curve Discrete Logarithm
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECPKC	Elliptic Curve Public-Key Cryptography
FEAL	Fast Data Encipherment Algorithm
FIPS	Federal Information Processing Standards
GF	Galois field
GNFS	Generalized Number Field Sieve
IDEA	International Data Encryption algorithm
IEEE	Institute of Electrical and Electronics Engineers.
IFP	Integer Factorization Problem

ISO	International Standards Organization
LUC	Lucas
MD	Message Digest
MIPS	Millions of Instructions Per Second
MPQS	Multiple Polynomial Quadratic Sieve
NIST	National Institute of Standards and Technology.
NBS	National Bureau of Standard
NSA	National Security Agency.
NFS	Number Field Sieve
PKI	Public-Key Infrastructure.
PKCS	Public-Key Cryptography Standards.
PKC	Public-key Cryptography
QS	Quadratic Sieve
RSA	Rivest, Shamir and Adleman.
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SK	Session key
SSL	Secure Socket Layer.
XTR	Compact Subgroup Trace Representation

CHAPTER I

INTRODUCTION

The Statement of Problem

The connectivity of computers and wireless communications make ways of protecting data and messages from tampering or reading important. Although the modern cryptography methods have been adopted widely, many models and systems are waiting for a new ideal method to optimize the following cryptosystem problems:

1- The Security: The secure algorithm must satisfy two conditions. First, the mathematical equations are so complex. Second, the cost or time required to recover the message or key is too much when using methods that are mathematically less complicated.

2- The Functionality: to meet various information security objectives.

3- The Performance: which refers to the efficiency of an algorithm in a particular mode of operation.

4- The Key Size: Number of bits required to store the key pairs and any system parameters.

5- The Bandwidth: The number of bits necessary to transfer an encrypted message or a signature.

Objectives of the Research

This research utilizes the attractive feature of the elliptic curve method as the functionality, the security and the small key size, and then enhances its performance and bandwidth. Therefore the research objectives are to:

1- **Improve the elliptic curve performance**: the performance of the elliptic curve method relies on algorithms that are necessary to accomplish the underlying finite field operations and the elliptic curve group operations. The curve operations are the full addition formula to add two points, doubling the curve points and the scalar multiplication of the elliptic curve group.

2- **Reduce the elliptic curve bandwidth**: there are four essential factors that control the elliptic curve bandwidth, namely the size of the elliptic curve coefficients, the elliptic curve base point, the general curve points and the size of the secrete key. The curve coefficients and the points coordinate are elements in the underlying finite field.

Importance of the Research

In the information technology age, the communications media are growing rapidly. The Internet encompasses more than 1,800,000 hosts and 15,000 networks (Brands, 1995). The electronic mail is gradually replacing conventional paper mail and messages, business through the Internet has become a homely behavior. Per contra; the nature of the Internet and the electronic medium allows effective scanning of a sensitive data using a sophisticated filtering software, credit card and debit card fraud that could cost online merchants billions of dollars over the next years. Therefore, the right solution for the communication security in general and the Internet security in particular will change the way business is conducted. One smart card could replace several cards, the wallet, the licenses and other important documents.

A cryptosystem or cipher system is a method or algorithm of disguising messages so that only certain people can see through the disguise. It is also the study of mathematical techniques related to aspects of information security. Hence cryptography is the heart of the information security, and many of the network security objectives can be satisfied by implementing an ideal cryptosystem such as (Smith, 1999):

- Secure communications without prior arrangements.
- Protect the electronic transactions against unknown attacks.
- Protect the traffic between trusted hosts.
- Protect the whole range of Internet software.
- Isolate a distributed network from outsiders.
- Protect the privacy and integrity of messages.
- Reliably identify who wrote a message or who is talking to you.

Thus the main goals of cryptography are (Menezes et al., 1996):

1- Privacy or confidentiality: To keep information secret from the unauthorized person.

2- Data integrity: To ensure information has not been altered by unauthorized or unknown means.

3- Authentication: This function applies to both entities and information itself. Two parties entering into a communication should identify each other.

4- Non-repudiation: preventing the denial of previous commitments or actions.

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, network protocol stack, socket interface, application software (Smith, 1999). Moreover, the cryptography techniques are necessary for wide range of applications can be categorized as follows:

- **The Internet applications**

  Secure electronic mail, home banking, Internet browsing, on-line financial services, electronic cash, credit card transactions and smart card.

- **Wireless Communications and Telecommunications**

  Pagers, cellular telephones, fax encryption, modems, secure telephones, Cable TV and pay-per-view.

Contributions of the Research

Several new techniques and algorithms are used to speed up the elliptic curve method computation and reduce the size of the transited parameters. The new approaches do not reduce the security, and the number of the elliptic curve base points is still very large and supports the users with very rich choices.

The contributions of this thesis can be summarized from the results of the study as follows:

1- A new full addition formula in the projective coordinate, where the analysis for this formula shows that the number of multiplications over GF (2^m) is reduced from 10 to nine general field element multiplications, thus this reduction will speed up the calculation about11 percent.

2- A new algorithms to find sparse base points, compress and decompress the sparse elements in *GF(q)* and compute the sparse multiplication over polynomial basis and normal basis.

3- A new group over *GF(p)* with a hard discrete logarithm problem, and a new algorithm to implement the group scalar multiplication.

Organization of the Dissertation

The dissertation has seven chapters, including this introductory chapter. The remaining chapters are:

Chapter II – Literature review covers the history of cryptography, basic definitions, public key cryptography and the famous cryptoanalysis methods. The chapter explains the two major problems that have been used in the public key cryptography; the first is the integer factorization problem which is used for the first time with RSA method, and the second problem is the discrete logarithm problem over the multiplication group of a finite field. The famous algorithms to solve these problems are clearly described. This chapter also discusses the extension of these problems for the new cryptography methods LUC and XTR.

Chapter III- Elliptic curve arithmetic operations introduces the underlying finite field algorithms, elliptic curve group operations, the elliptic curve classifications and the implementation of the basic curve operations. The curve operations are considered the heart of elliptic curve protocols and applications. Thus, the most known and efficient algorithms for the underlying field and elliptic curve group are discussed, which includes adding, squaring, multiplication, Inversion and the scalar multiplication for the elliptic curve group elements over prime and binary fields. Elliptic curve classifications are very important to study the elliptic curve discrete logarithm problem and to select a secure and efficient curve parameters. The chapter ends by the numerical comparison for different types of finite field, key size and curve coefficient.

Chapter IV- Discrete logarithm problem over new groups contains three parts, the first explains the famous algorithms to solve the elliptic curve discrete problem and the necessary conditions to select a secure curves. The second part discusses methods to find a nearly prime and large order for the elliptic curve group, thus to ensure the difficulty of solving the curve problem. The third part introduces two new groups to exam the discrete logarithm problem over them, where the discrete logarithm problem over the first can be solved easily, but the primary analysis for the second group shows the difficulty of solving the discrete logarithm problem over it.