UNIVERSITI PUTRA MALAYSIA

A NEW CRYPTOSYSTEM BASED ON DECIMAL NUMBERS AND NONLINEAR FUNCTION

RAND QUSAY ALFARIS

IPM 2009 5

A NEW CRYPTOSYSTEM BASED ON DECIMAL NUMBERS AND NONLINEAR FUNCTION

By

RAND QUSAY ALFARIS

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

June 2009

To you
Mother and Father

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

A NEW CRYPTOSYSTEM BASED ON DECIMAL NUMBERS AND NONLINEAR FUNCTION

By

RAND QUSAY ALFARIS

June 2009

Chairman: Mohamed Rushdan Md Said, PhD

Institute: Institute for Mathematical Research

We introduce a new cryptosystem, with new digital signature procedure. This cryptosystem is based on decimal numbers and nonlinear function. Unlike other cryptosystems, this system does not depend on prime or integer numbers and it does not depend on group structure, finite field or discrete logarithmic equation. The idea is about using decimal numbers and thus the only integer number will be the plaintext. A secret key is shared between Alice and Bob to construct their decimal public keys, so that, we can say this cryptosystem is symmetric and asymmetric. We choose to distribute the secret key through the classic Diffie-Hellman protocol after introducing some modification on it; this modification depends on the extension of the theory of the modulus to be applicable on the real numbers. We prove there is no loss of any bit of information when we use the decimal numbers during the encryption and the decryption by introducing the rounding off

concept as a function. This function plays the primary role in proving a new theorem called "Rounding theorem". A new theory for the security is established, where basically, it depends on the properties of the decimal numbers and the cumulative and truncation errors that will occur during the attack, because every attack requires solving a system of non-linear equations. The decimal cryptosystem does not depend on large numbers because it deals with numbers between zero and one. Therefore, this cryptosystem can be considered faster than the known cryptosystems.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk ijazah Doctor of Philosophy

SATU CRYPTOSYSTEM YANG BARU BERDASARKAN NOMBOR PERPULUHAN DAN TAK LINER FUNGSI

Oleh

RAND QUSAY ALFARIS

Jun 2009

Pengerusi: Mohamed Rushdan Md Said, Ph.D.

Institut: Institut Penyelidikan Matematik

Kita memperkenalkan pembaharuan kriptosistem, iaitu prosedur tandatangan digital baru. Kriptosistem ini berasaskan nombor perpuluhan dan fungsi tak linear. Berbeza dengan kriptosistem yang lain, sistem ini tidak bergantung kepada nombor perdana atau nombor-nombor bulat dan juga tidak bergantung kepada struktur kumpulan, bidang terhingga atau persamaan logaritma diskrit. Ideanya adalah mengenai penggunaan nombor perpuluhan dan nombor bulat yang hanya akan menjadi plaintext. Kunci rahsia adalah perkongsian antara Alice dan Bob untuk membina kunci-kunci awam dalam bentuk perpuluhan supaya kriptosistem ini boleh dikatakan simetri dan tak simetri. Kita memilih untuk mengedarkan kunci rahsia melalui skim klasik Diffie-Hellman selepas memperkenalkan beberapa

pengubahsuaian ke atasnya; perubahan ini bergantung kepada sambungan kepada teori modulus yang dapat disesuaikan pada angka sebenar. Kita dapat membuktikan bahawa tidak terdapat kehilangan sebarang bit pada maklumat apabila kita menggunakan nombor-nombor perpuluhan sepanjang enkripsi dan dekripsi dengan memperkenalkan konsep pembundaran sebagai satu fungsi, fungsi ini memainkan peranan utama dalam pembuktian teorem baru yang dipanggil "Rounding teorem". Satu teori baru untuk keselamatan telah ditubuhkan, pada asasnya, ia bergantung kepada ciri-ciri nombor perpuluhan dan kumulatif dan ralat pangkasan yang akan berlaku semasa serangan kerana setiap serangan menghendaki penyelesaian sistem persamaan tak linear. Kriptosistem dalam bentuk perpuluhan tidak bergantung kepada nombor yang besar daripada pandangan nilai nombor kerana ia menggunakan nombor antara sifar dan satu. Oleh itu, kriptosistem ini boleh dianggap lebih cepat daripada kriptosistem yang diketahui.

ACKNOWLEDGMENTS

I give my humble thanks to God, the creator of the the universes for giving me the strength and patience to complete this thesis. Only by His grace and mercy this thesis can be completed.

I would like to express my sincere gratitude to my supervisor Assoc. Prof. Dr. ***Mohamed Rushdan Md said***, Head of Laboratory of Theoretical Research, Institute for Mathematical Research, UPM, for his invaluable guidance, supervision, support, patience and continuous encouragement that helps me to work hard during my study. My gratitude also go to the members of the supervisory committee, Assoc. Prof. Dr. Mohamed Othman, Department of Communication Technology and Network, Faculty of Science and Information Technology UPM, and Assoc. Prof. Dr. Fudziah Ismail, Head of Mathematics Department, Faculty of Science, UPM, for their helpful, comments, advices and kindness.

Many people in the Institute for Mathematical Research I need to thank them for their help and guidance, especially, I would like to thank Mr. Muhamad Rezal Kamel Ariffin for sharing with me his knowledge, and as an outcome for working together, we could put our first paper under the supervision of Assoc. Prof. Dr. Mohamed Rushdan.

I wish to thank my brothers Ali and Munaf, my sister Rafeef and all of my friends for their love and support.

Most of all, I am forever indebted to my parents, for their endless encouragement and their love to let me handle the far way distance and the difficulties during my study. I pray to God to help me to give them back even if a small part of their sacrifices.

This thesis was submitted to the Senate of University Putra Malaysia and has been accepted as fulfilment of the requirement for the Degree of Doctor of Philosophy.

The members of the supervisory Committee were as follows:

Mohd Rushdan Md Said, PhD
Associate Professor
Institute for Mathematical Research
University Putra Malaysia
(Chairperson)

Mohamed Othman, PhD
Associate Professor
Department of Communication Technology and Network
Faculty of Science and Information Technology
University Putra Malaysia
(Member)

Fudziah Ismail, PhD
Associate Professor
Department of Mathematics
Faculty of Science
University Putra Malaysia
(Member)

HASANAH MOHD. GHAZALI, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 16 October 2009

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

RAND QUSAY ALFARIS

Date: 24 August 2009

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

1.1 Overview

In this research, we present a new cryptosystem and we call it "The Decimal Cryptosystem". We know that constructing a new cryptosystem is not easy as any new cryptosystem must have its own significant contribution in secure communications. The purpose of this cryptosystem is to get secure, fast communication that does not depend on the size of the key.

The Decimal Cryptosystem depends on decimal numbers as the base for constructing the keys. This cryptosystem does not depend on prime or integer numbers and it does not depend on group structure, finite field.

The public key of the decimal cryptosystem is formalized by using nonlinear function that produce only decimal numbers and it depends on two components. The first component is the private key for each user and the second component is the secret key which must be shared among the users. So that this cryptosystem is mixed between the symmetric and asymmetric system.

We choose to distribute the secret key through the classic Diffie-Hellman protocol after introducing a modification on it to convert the large integer numbers to decimal numbers with doubling the protection of the exchanging secret key. The classic Diffie-Hellman protocol will be modified through an extended theory of the congruence.

We prove there is no loss of any bit of information when we use the decimal numbers during the encryption and the decryption by introducing the rounding off concept as a function. This function plays the primary role in proving a new theorem called "Rounding theorem".

A new direction for the theory of security is established. Basically, it depends on the cumulative and truncation errors that will occur during the attack. With a cryptosystem that depends on decimal numbers, any well known method for attacking must involve numerical methods, each of which as we know has a limit for accuracy. Therefore, using numerical methods will not give the exact solution, since there is always an error called "cumulative error" because of the truncation on the digits of the decimal numbers. Normally, in the integer number concept, the size of the key determines how large the number is. The situation is different in the decimal cryptosystem, no matter how big the size of the key, still the numbers involved are small because it deals with numbers between zero and one. Therefore, the decimal cryptosystem can be considered faster than the current cryptosystems because the amount of time needed for implementing the arithmetic calculations on decimal numbers is much less than the time needed for implementations involving the large integer numbers.

To avoid any misunderstanding, we use the term "decimal number" as defined in set theory, as in Hrbacek and Jech (1999), in time, the term "decimal number" means "integer number" in computer theory. For example, the number 4529 is defined as decimal number from the viewpoint of the computer languages, as in Cohoon and Davidson (1997). We will give the definition of the decimal numbers in chapter 5.

1.2 Problem Statements

Most of the existing cryptosystems are based on group structures, finite fields and/or discrete logarithmic equation and deal only with integer numbers. The security of these cryptosystems mostly depends on the key size such that, the much faster computers take a longer time to find the right key, as in Schneier (1995). This new cryptosystem does not deal with integers and it does not depend on group structure or finite field. Instead, it depends on non-linear functions and decimal numbers and on their properties.

Using the decimal numbers gives the risk of losing some information of the plaintext. As we all know the decimal numbers are not specific numbers as the integers because there is always fractional part in a decimal number. We mean by the specific numbers is, when we talk about the number "91076310985345423" then there is no doubt that the beginning of the number is the digit "9" and the end of the number is the digit "3". But when we talk about the number, "0.91076310985345423", then we can consider that the beginning of the number is the first digit after the decimal point but we cannot be sure that the end of the number is "3". We will always have the question: what was the digit after "3" before terminating the number? The specific number means that there is known position for the ones, tens, hundreds and so on, and there are specific first and last digits. For decimal numbers there is no such specification. The main concern is when we talk about the recurring type such as 0.47474747... and the nonrecurring or not exact type such as *pi*.

Despite this fact, the questions are, is there a possibility for constructing a cryptosystem that depends on the decimal numbers? What is the strength of using the decimal number in cryptography? We give the answers to these two main ques-

tions, and we put the proofs for the validity of the encryption and the decryption algorithms. We show that there is neither cumulative error nor truncation error in applying the algorithms, but there is a rounding off. For this purpose, we design the function that defines the rounding off concept, which plays the main role in proving the theorem called "Rounding theorem". This theorem gives the answers to why there is no error during the encryption/decryption of this new decimal cryptosystem.

The security of this new cryptosystem depends on two parts. The first part based on using one of the nonlinear functions of two variables that produces only the decimal numbers. This part of the security depends on the fact that there is no unique solution for such equations unless there is a system of two equations for these unknown variables. We hide this function under the representation, which we call Jay function or J-function. The unknown variables are decimal numbers and that means the approximation will not work. The attacker needs the exact value for the key with the same number of digits of the decimal number.

This strong point does not exist in other cryptosystems that depend on integer numbers. If the secret key in one of these cryptosystems was 76 then if the attacker found it, then it will be neither 77 nor 75, but the exact key 76. The situation is different in the decimal cryptosystem; there is a decimal number so there are digits after the decimal point, and the attacker does not really know how many digits he will lose during the approximation, if the key was 0.652491, then the attacker will find the difficulty of finding this key with same digits. The methods of recovering the keys in the decimal cryptosystem should pass through the numerical methods then, definitely, the attacker will face the cumulative and the truncation errors. Therefore, the attacker will not get the same decimal number.

On the other hand, there are no numerical methods in applying the algorithms of this new decimal cryptosystem. We can call it as 'one way operation'; the user applies the algorithms of the decimal cryptosystem without losing any bit of information, but the attacker will lose some of the information because of the truncation. We introduce all possible attacks to this cryptosystem. The second part of the security depends on introducing modification on classic Diffie-Hellman key exchange protocol. This modification depends on the extended theory of the congruence, which will cover the set of the real numbers. We calculate the time needed to do the communications (encryption/decryption) in decimal cryptosystem and we test the results in comparing with two cryptosystems, ElGamal and RSA, we find that the new decimal cryptosystem is much faster even if we implement ElGamal and RSA with very short key size.

1.3 Research Objective

The objective of the decimal cryptosystem is:

- To avoid dealing with integers or prime numbers.
- To avoid dealing with the usual algorithms of the security, and creating new algorithms that do not depend on the size of the key or the complexity of the algorithms. But they depend on the error that would occur when using any well-known method for attacks.
- Dealing with decimal numbers that belong to uncountable set of numbers.
- Create a fast medium of communications because the decimal number is a small number no matter how many digits it has.

1.4 The Contribution of the Research

In this research, using the decimal numbers in cryptography field is the main contribution. We move from the integer numbers to the decimal numbers because of the advantages of this field of numbers in secure communications. The time that is needed to implement the algorithms that depend on decimal numbers is not noticeable when compared to the time that it is needed to implement algorithms that depend on integer numbers. On the contrary, the time needed increases exponentially with the increase of the size of the key in case of integers. For the decimal key, the number stays less than 1, however much the key size increases which the factor that does not affect the time to carry out the calculations.

The second contribution is in proving that the decimal numbers do not affect the validity of the secret communications, by theorizing the rounding theorem. By using the rounding theorem is not restricted to the decimal cryptosystem but it is also applicable to any protocol that depends on the decimal numbers.

In this research, we generalize the theory of the congruence for the first time. The generalization is in extending the congruence theory to be applicable on the real numbers. Until now the theory of congruence is restricted to the ring of integers only.

The new direction in the theory of the security is our last contribution in this research. This direction is based on involving the numerical methods with the classic methods of the attack. This produces commutative error in each step of the attack because all of the algorithms in the decimal cryptosystem is based on nonlinear function and at least three unknown keys.

1.5 Scope and Thesis Organization

1.5.1 The Scope of the Research

We present four main results: Constructing new cryptosystem with new digital signature procedure based on decimal numbers, and we derive the algorithms of the encryption and the decryption. Theorizing and then proving that there is no lost of any bit of information because there is neither cumulative error nor truncation error for the legitimate users. We achieve this result by designing a mathematical closed form function for the rounding off concept and then theorizing and proving the Rounding theorem. Modifying the classic Diffie-Hellman protocol is done through extending the theory of the congruence. The last result is establishing a new direction for the security through involving the numerical systems of nonlinear equations of multiple unknown variables with each method of attack.

1.5.2 Thesis Organization

The thesis is organized as follows. Chapter one is the introduction, which contain the overview, research statement, research objective and the contribution of the research.

The literature review is in Chapter two where we review the topics that are considered as the bases of this research, namely the three topics; Diffie-Hellman protocol, ElGamal cryptosystem and the congruence theory. We refer to Bisseling and Flesch (2006), Cormen et al. (2001a), Lenstra et al. (1990), Pomerance (1996), Kleinjung (2006), Shor (1994), Diffie and Hellman (1976), Pohlig and Hellman (1978), Pietrzak (2005), Maurer and Wolf (2000), ElGamal (1985), Wu et al. (2001), Verkhovsky (2008), Nagell (1951), Hejhal et al. (1999), Hrbacek and Jech

(1999), Kenneth and Rosen (1990[a,b]) and Apostol (2000).

We introduce the extension to the theory of the congruence in chapter three based on extending the existing theorems of the congruence. (Nagell, 1951), (Niven and Zuckerman, 1980), (Hejhal et al., 1999), (Cormen et al., 2001a), (Burton, 1989), (Conway and Guy, 1996), and (Gilbert and Gilbert, 2005).

Chapter four is the modification of Diffie-Hellman protocol and the construction of the cryptosystem, where we describe the secret, private and public keys. In addition, we introduce the algorithms of the encryption and decryption and the algorithms of the new digital signature procedure. (Beth and Gollmann, 1989) and (ElGamal, 1985). The comparison between the decimal cryptosystem against the ElGamal cryptosystem and the decimal cryptosystem against RSA is introduced in this chapter, we refer to (ElGamal, 1985) and (Rivest et al., 1978). For modifying Diffie-Hellman protocol we refer to Diffie and Hellman (1976) and Séroul (2000).

In Chapter Five, we begin with the definition of the decimal numbers as in Hrbacek and Jech (1999), where we choose to illustrate it here, because it is related to the contents of this chapter more than it relates to chapter Four. We discuss the rounding off of the decimal cryptosystem, and we show that there is no truncation error when the partners apply the encryption/decryption algorithms of this cryptosystem. We introduce the proof for the theorem called "Rounding theorem" which is the main step to prove of receiving the deciphertext (the plaintext after decryption) without any error. For this purpose, we design a new function called "Rounding off Function" which plays the main role in proving this theorem. Beside, we prove the decryption algorithm of this new decimal cryptosystem mathematically and from the viewpoint of the computer theory. We mostly refer

to Anderson and Feil (2005), Hrbacek and Jech (1999) and Schumer (1996).

Chapter six is for the security where we discuss the length of the plaintext and the size of the key and the relation between them in the decimal cryptosystem. We Introduce the possible methods of the attacks and we show that these method will fail with the decimal cryptosystem because of the decimal numbers. (Schumer, 1996), (Menezes et al., 1996), (Katsuyuki and Tsuyoshi, 2004) and (Vasilenko, 2007).

Chapter seven is allocated for the conclusion and efficiency aspects of this cryptosystem and the future work.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

Since the early seventies of the last century, cryptosystems depend on integer numbers and prime numbers with large size keys in order to give high level security. This security is guaranteed by the incapability of the current computer systems to identify the algorithms of the cryptosystems in a short time, due to complexity of the algorithms. However, as the revolution of the communications is growing, these cryptosystems will fail once high speed computer systems are developed.

As of 2005, in RSA, the largest number factored by a general-purpose factoring algorithm was 663 bits long, (Bisseling and Flesch, 2006). RSA keys are typically 1024–2048 bits long, (Cormen et al., 2001b). some experts believe that by applying fast factorization algorithms that used the number field sieve (NFS), (Lenstra et al., 1990), 1024-bit keys may become breakable in the near future.

The general number field sieve (GNFS) which is the generalization of the "special number field sieve (SNFS)" is the most efficient classical algorithm known for factoring integers larger than 100 digits. Its complexity for factoring an integer n, consisting of $\log n$ bits) is of the form

$$O\left(e^{(c+o(1))(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}}\right) = L_n\left[1/3, c\right] \tag{2.1}$$

for a constant c which depends on the complexity measure and on the variant of the algorithm, (Pomerance, 1996) and (Kleinjung, 2006). According to that, the specialists see that 4096-bit keys could be broken in the foreseeable future.

Most implementations are split three ways: polynomial selection, sieving, and final processing. The gold-standard implementation until 2007 was a suite of software developed and distributed by National Research Institute for Mathematics and Computer Science which is one of the leading European research centers in the field of mathematics and theoretical computer science in Netherlands, which was available only under a relatively restrictive license. In 2007, it has developed a faster implementation of final processing as part of GNFS, which is public-domain. General number field sieve, however, can only run on a single symmetric multiprocessing (SMP) computer, while National Research Institute for Mathematics and Computer Science's implementation can be distributed among several nodes in a cluster with a sufficiently fast interconnect.

A theoretical hardware device named TWIRL and described by Shamir and Tromer in 2003 called into question the security of 1024 bit keys. It is currently recommended that the size of the key be at least 2048 bits long.

On the other front, in 1994, the mathematician Peter Shor published Shor's algorithm, (Shor, 1994), showing that a quantum computer could in principle perform the integer factorization in polynomial time.

Shor's algorithm: is a quantum algorithm for factoring an integer N in $O((\log N)^3)$ time and $O(\log N)$ space.

Shor, demonstrates that integer factorization is in the complexity class Bounded error, Quantum, Polynomial time (BQP). This is exponentially faster than the best-known classical factoring algorithm, the general number field sieve, which works in sub exponential time about $O(2^{(\log N)^{1/3}})$.

The bottom line is, the security of the cryptosystems that depends on the size of the key is now under serious threat. We need to think of alternative solutions for the security and to build a secure cryptosystems that does not depend on the race between increasing the key size and high speed computers.

There is attempt to use a subset of the decimal numbers in cryptography which is the transcendental numbers, (Pieprzyk et al., 1996). We will highlight it in the next section.

In this research we introduce a new direction in cryptography by introducing a cryptosystem which we call "The Decimal cryptosystem", where the security depends neither on integer numbers, the key size nor on the prime factorization. Instead, it depends on decimal numbers which belong to the interval $(0, 1)$. The base of this cryptosystem depends on ElGamal cryptosystem, Diffie-Hellman protocol and the theory of the congruence which we will review in this chapter.

2.2 Transcendental Numbers

The early attempt of using the decimal numbers in cryptography was in 1996 by Pieprzyk et al. (1996). This attempt was not about using the decimal numbers in general as we are proposing in this research, but it was exclusive on a subset of irrational numbers which is called the "Transcendental Numbers".

A ***Transcendental Number*** is a (possibly complex) number that is not the root of any integer polynomial, meaning that it is not an algebraic number of any degree. Every real transcendental number must also be irrational, since a rational number is, by definition, an algebraic number of degree one, (Baker, 1975). In