UNIVERSITI PUTRA MALAYSIA

EXTENTION AND CRYPTANALYSIS OF GOLDEN CRYPTOGRAPHY

MOHAMMAD TAHGHIGHI SHARABYAN

FSKTM 2015 18

EXTENTION AND CRYPTANALYSIS OF GOLDEN CRYPTOGRAPHY

By

MOHAMMAD TAHGHIGHI SHARABYAN

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

August 2015

DEDICATIONS

To my dear parents and My lovely family

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

EXTENSION AND CRYPTANALYSIS OF GOLDEN CRYPTOGRAPHY

By

MOHAMMAD TAHGHIGHI SHARABYAN

August 2015

Chair: Associate Professor Azmi Jaafar, PhD
Faculty: Computer Science and Information Technology

There are some symmetric cryptosystems which use matrices in the encryption and decryption of initial data and the golden cryptosystem (GC) is one of the cryptosystems. It uses a kind of matrices that is normally called the golden matrices, which is a generalization of the Fibonacci Q-matrices for continuous domain. The GC, like other matrix cryptosystems, cannot resist against chosen-plaintext attack. On the other hand, the encryption algorithm of GC is more suitable for textual data and cannot be directly applied to images. This is because image data usually have special features such as bulk capacity, high redundancy, and high correlation among pixels that impose special requirements on the encryption technique used. The problems of golden matrix mentioned are the motivation for the proposal of more secured GC.

In this thesis, the mathematical technique was used to check the security of two extend versions of GC; the GC using k-Fibonacci number (KGC) and GC using Hadamard product (HGC). Utilizing chosen-plaintext attack for both extended versions (the golden cryptosystem using k-Fibonacci number and Hadamard product) are proven not secured. Then a new extension to the original GC using discrete logarithm problem and hash function (GCHDLP) was proposed and the tests have shown that these versions of GC can resist the four basic attacks; the chosen-plaintext attack, known-plaintext attack, the ciphertext-only attack, and chosen-ciphertext attack.

Finally, the experimental results, using several images (Lena, Nike, Micky, and Damavand) and three measuring factors were evaluated. These measuring factors were the maximum deviation measure (M1), the correlation coefficient measure (M2), and the irregular deviation measure (M3). The proposed method GCHDLP can encrypt identical plaintext blocks to totally different ciphertext blocks, whereas the original GC cipher cannot do so. Thus, the proposed method has advantages in hiding data patterns over original GC.

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

KRIPTANALISIS DAN UNJURAN BAGI KRIPTOGRAFI EMAS

Oleh

MOHAMMAD TAHGHIGHI SHARABYAN

Ogos 2015

Pengerusi: Professor Madya Azmi Jaafar, PhD
Fakulti: Sains Komputer dan Teknologi Maklumat

Terdapat beberapa sistem kripto simetri yang menggunakan matriks dalam penyulitan dan penyahsulitan data awal dan Sistem Kripto Emas (GC) adalah salah satu daripada sistem kripto tersebut. Ia menggunakan sejenis matriks yang dipanggil matriks emas, yang merupakan generalisasi daripada Fibonacci Q- matriks untuk domain yang berterusan. Kebanyakan matriks sistem kripto seperti GC tidak dapat bertahan daripada serangan pilihan teks biasa. Di samping itu, algoritma penyulitan GC adalah lebih sesuai digunakan untuk data-data tekstual dan tidak sesuai mahupun boleh digunakan pada imej. Ini adalah kerana data imej mempunyai ciri-ciri khas seperti keupayaan pukal, kelewahan tinggi dan korelasi yang tinggi di antara piksel yang mengenakan syarat-syarat khas mengenai teknik penyulitan yang digunakan. Masalah-maslah matriks emas diatas adalah motivasi kepada cadangan sistem kripto emas yang lebih terjamin.

Dalam tesis ini, teknik matematik digunakan untuk memeriksa keselamatan dua versi GC iaitu sistem kripto emas menggunakan nombor k - Fibonacci (KGC) dan sistem kripto emas menggunakan Hadamard produk (HGC). Penggunaan serangan pilihan teks biasa ke atas kedua-dua versi lanjutan sistem kripto emas menerusi nombor k - Fibonacci dan produk Hadamard telah dibuktikan sebagai tidak selamat. Maka, sistem kripto emas yang baru menggunakan masalah logaritma diskret dan fungsi hash (GCHDLP) dicadangkan dan ujian keatasnya telah menunjukkan bahawa ia dapat bertahan terhadap empat serangan asas, iaitu serangan pilihan teks biasa, serangan teks biasa yang kenal, serangan teks sifer dan serangan pilihan teks sifer.

Keputusan eksperimen menggunakan beberapa imej (Lena, Nike, Micky dan Damavand) dan tiga faktor pengukur dipertimbangkan dan dinilai. Faktor-faktor ini adalah ukuran maksimum sisihan (M1), ukuran pekali korelasi (M2) dan ukuran sisihan yang tidak teratur (M3). Kaedah GCHDLP yang dicadangkan boleh menyulitkan blok teks biasa yang serupa dengan blok teks sifer yang jauh berbeza dimana sifer GC asal tidak boleh lakukannya. Maka, kaedah yang dicadangkan mempunyai kelebihan dalam menyembunyikan corak data berbanding GC asal.

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Associate Professor Dr. Azmi Jaafar for his patience and helpful supervision, guidance and valuable suggestions. I also thank the committee members Prof. Dr. Ramlan Mahmod and Prof. Dr. Mohammad Rushdan Md. Said for their efforts and valuable comments.

Finally, I am grateful to the Faculty of Computer Science and Information Technology, School of Graduate studies and the library of the University Putra Malysia, for providing a good environment for studying and researching.

Mohammad Tahghighi Sharabyan

I certify that a Thesis Examination Committee has met on 10 August 2015 to conduct the final examination of Mohammad Tahghighi Sharabyan on his thesis entitled "Extension and Cryptanalysis of Golden Cryptography" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Abu Bakar bin Md Sultan, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Nur Izura binti Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Zuriati binti Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Adnan Abdul-Aziz Gutub, PhD
Professor
Umm Al-Qura University
Saudi Arabia
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 22 September 2015

This thesis was submitted to the Senate of Universiti 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:

Azmi Jaafar, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Ramlan Mahmod, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Mohammad Rushdan Md. Said, PhD
Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

BUJANG BIN KIM HUAT, Ph.D.
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by Graduate Student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Unievrsiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ______________________ Date: ______________________

Name and Matric No: ______________________

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsbilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature:________________________

Name of Chairman of Supervisory Committee
Associate Professor Azmi Jaafar, PhD

Signature:________________________

Name of Member of Supervisory Committee
Professor Ramlan Mahmod, PhD

Signature:________________________

Name of Member of Supervisory Committee
Professor Mohammad Rushdan Md. Said, PhD

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCM	Combined Cipher Machine
CFB	The Cipher Feedback
CTR	Counter
CWC	Carter-Wegman+CTR
DES	Data Encryption Standard
DLP	Discrete Logarithm Problem
FIPS PUB	Federal Information Processing Standards Publication
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptosystem
ELC	Extended Lucas Cube
GC	Golden Cryptography
GCM	Galuis/ Counter Mode
GCHDLP	Golden Cryptography using Hash Function and Dlp algorithm
HF	Hash Function
HFE	Hidden Fields Equations
HGC	Extension of GC by using Hadamard product
IAPM	Integrity Aware Parallelizable Mode
IV	Initialization Vector
KGA	Keystrem Generation Algorithm
KGC	Extension of GC by using k-Fibonacci number
KSA	Key Scheduling Algorithm
LFR	Linear Feedback Shift Register
MD4	Message Digest 4
MFE	Medium Field Equation
MIC	Message Integrity Code
NIST	National Institute of Standards and Technology
OCB	Offset Codebook
OFB	Output Feedback
OTP	One Time Pad
PIN	Personals Identification Number
PMI	Perturbed Matsumoto-Imai
PRNG	Pseudo Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SPN	Substitution-Permutation Network
SSL	Secure Sockets Layer
TDE	Triple Data Encryption
TTM	Tame Transformation Methods
WEP	Wired Equivalent Privacy
R-G-B	Red Green Blue

CHAPTER 1

INTRODUCTION

1.1 Cryptography

Cryptography is a process for encrypting and decrypting information using pure mathematics, computer science, and engineering. Making the messages secure via cryptography has a long history (Menezes et al., 1997). Julius Caesar (100-44 B. C.) is well-known for creating one of the earliest cryptographic systems to send secret military messages to his generals. But history has shown that a big principal problem had been limiting the widespread use of cryptography, i.e., the key management. The term "key" refers to a numerical value used by an algorithm to change the information, make it secure and visible just to those who have the corresponding key for recovering the information. As a result, the term "key management" refers to managing the keys securely and provide them to the users where and when they are required. In fact, cryptography is used to hide information, so it is not only used by spies but also for phone, fax and e-mail communications, bank transactions, bank account security, personal identification number (PIN), passwords, and credit card transactions on the web. It is also used for various information security issues such as electronic signatures, which are basically used to prove the identity of the sender of the message. The goal of cryptography is to provide the possibility of exchanging a message between a sender and a receiver in a way that only these two persons can understand it. In this manner, the ways of exchanging the message are unlimited, but here it can be concerned with the methods of altering the text in such way that makes the receiver able to undo the alteration and to discover the original text. The original text is usually called "plaintext" and the altered text is called "ciphertext" and the conversion from plaintext to ciphertext is called "encoding" or "enciphering". The reverse operation is called "decoding" or "deciphering". If an unintended secret message is tried to be read and the encoding method is not known, then the code will crack. Generally, there are two kinds of cryptography: symmetric and asymmetric cryptography.

1. Symmetric cryptography: Symmetric-key cryptography is useful to supply data (Scheneier, 1996) on general communication networks such as internet confidentiality. That involves encryption of a plaintext message "P" by a symmetric-key algorithm (cipher) and a secret key K. When the encrypted message (ciphertext) is sent, the receiver decrypts it using the same cipher

and secret key. Symmetric-key ciphers usually have an iterated round structure, i.e. a short sequence of operations (called a "round") is repeated on the plaintext block to compute the ciphertext (Scheneier, 1996). "The input of a round consists of the output of the previous round and one or more subkeys, which are derived from the secret key. Common round operations include table lookups, modular addition (subtraction), logical operations, shifts, rotates, multiplication, and bit permutations (Scheneier, 1996)". Being fast and suitable for processing large streams of data is the advantage of symmetric cryptography algorithms. The disadvantage of symmetric cryptography is that it presumes two parties have agreed on a key and able to exchange that key in a secure manner before the communication (Ugus et al., 2007). This is a significant challenge.

2. Asymmetric cryptosystem: Public key cryptography is applied often in electronic commerce to provide an authentication secure communication. The most common cryptosystems, Rivest, Shamir, and Adleman (RSA) and elliptic curve cryptosystems (ECC), are established based on the trouble of integer factorization and discrete logarithm. Meliorating factorization algorithm and calculation power request greater bit size in RSA key. Actually the suggested key size is 1024 bits which may increase to 4096 bits (Schneier and Sutherland, 1995). Greater key size makes RSA less effective for real applications. Compared to RSA, ECC is more effective, but it is the shortest signature which consists 320 of bits that are long for many appliances (Johnson et al., 2001). Unfortunately the mentioned systems have such disadvantages, and are not broken yet. Peter Shor (Shor, 1999) found a polynomial time algorithm for integer factorization and calculation of discrete logarithm for quantum computers in 1999. Thus, the cryptosystems with the mentioned troubles were no longer secure. There are many powerful motivations for developing the public key cryptosystems based on troubles that are secure on quantum and conventional computers. Multivarious cryptography can be an attainable choice for quantum and conventional computers. In multivarious cryptography, the public key cryptosystem is based on the trouble of solving the scheme of nonlinear equations that is proven to be NP-complete. The first practical kind of this cryptosystem was recommended by T. Matsumoto and H. Imai, (1988) and it is called message integrity code (MIC). The MIC cryptosystem was built by hiding a monomial x^{2^l+1} of two invertible affine transformations. This cryptosystem was more effective than RSA and ECC, but Patarin has broken it in 1995(Patarin, 1995). In 1996 he presented a generalization

of MIC cryptosystem called hidden fields equations (HFE) (Patarin, 1996). Anyway, the secret key computation of HFE was not sufficiently effective in the original MIC cryptosystem. In 1999 the chief model of HFE was broken (Kipnis and Shamir, 1999). The attack has applied this simple matter in which every homogeneous quadratic multivarious polynomial has a matrix display. By using the matrix display, a vastly defined system of equations will be obtained which can be deciphered by re-linearization (Kipnis and Shamir, 1999). Some other possible attacks on the HFE scheme have been found in (Courtois, 2001), (Courtois, 2003) and (Faugere and Joux, 2003). A few cryptosystems known as Dragons with multivarious polynomials of a whole degree 3 or 4 in public key were made by Patrin (instead of 2) which were more secure and efficient. In Dragon cryptosystem, the public key is a mixed of total degree 3 that is quadratic in plaintext variables and linear in ciphertext variables. Briefly, Dragon scheme with one hidden monomial was found to be not secure, hence the public key program based on the form of tame transformation methods (TTM) was recommended in (Moh, 1999). This plan was broken in (Goubin and Courtois, 2000); in which the cryptanalysis was decreased to an instance of Min-Rank trouble where it can be solved within an acceptable period. Ding (Ding, 2004) has suggested a perturbed kind of MIC cryptosystem which was named perturbed Matsumoto-Imai (PMI). The PMI system tries to increase the complication of the secret key calculation for increasing security by applying a system of r arbitrary quadratic equations over F_q with the assumption that $r << n$, where n is the bit size. The PMI system was broken by Fouque, Granboulan, and Stern (Fouque et al., 2005). The trick of the attack was the use of differential cryptanalysis to decrease the PMI system to MIC. Medium field equation (MFE) is a cryptosystem which has been proposed by (Wang et al., 2006) and Ding (Ding et al., 2007) in which a high order linearization equation attack has broken it. Also, there is a useful introduction of hidden monomial cryptosystems in reference(Koblitz, 1998). Making a secure and effective multivarious public key cryptosystem is still a challenge for researchers in recent years. This thesis focuses on the "Matrix cryptography". Most of these cryptosystems are in the symmetric category but in order to increase the security of above-mentioned cryptosystems, symmetric algorithms are most often mixed with public key algorithms to get a mix of security and speed. One of the cryptosystems is golden cryptography that will be introduced in the next section.

1.2 Golden Cryptography

Fibonacci number is one of the interesting recurrence relations with so many applications in science. For example Fibonacci numbers are used in the analysis of financial markets, in strategies such as Fibonacci retracement, and also used in computer algorithms such as the Fibonacci search technique and Fibonacci heap data structure. The simple recursive property of Fibonacci numbers has also inspired a family of recursive graphs which are called Fibonacci cubes and are useful for interconnecting parallel and distributed systems. But, probably the wonderful application of these numbers is in cryptography which was introduced by Stakhov (Stakhov, 2007). He has considered golden matrices as a new type of square matrices. These are a generalization of the classical Fibonacci Q-matrix for uninterrupted domain. The golden matrices are useful to create symmetric cryptosystem called golden cryptography, which is the main focus of this thesis. In cryptography, every simple and fast method for technical realization will be considered as a good method in science. Stakhov's method has proven that this cryptosystem is very fast to encrypt initial data. Some authors try to extend this method using other recurrence relations like Lucas and extended Lucas cube (ElC) or other operations such as Hadamard product (Ernastuti et al., 2010; Nally, 2007). Stakhov's method simply can be defined as below:

According to Fibonacci numbers, the Fibonacci matrix is defined as

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad Q^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad Q^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}, \cdots Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \quad (1.1)$$

where $n = 0, \pm1, \pm2, \pm3, \cdots, F_{n-1}, F_n, F_{n+1}$ are Fibonacci numbers given by the following recurrence relation:
$F_{n+1} = F_n + F_{n-1}$ (Johnson, 2008; Freixas and Kurz, 2013).

For any real number x, the *Q-matrices* is defined by

$$Q^{2x} = \begin{pmatrix} cF_s(2x+1) & sF_s(2x) \\ sF_s(2x) & cF_s(2x-1) \end{pmatrix}, \quad (1.2)$$

$$Q^{2x+1} = \begin{pmatrix} sF_s(2x+2) & cF_s(2x+1) \\ cF_s(2x+1) & sF_s(2x) \end{pmatrix}. \quad (1.3)$$

where

$$sF_s(x) = \frac{\tau^x - \tau^{-x}}{\sqrt{5}}, \tag{1.4}$$

$$cF_s(x) = \frac{\tau^x + \tau^{-x}}{\sqrt{5}}, \tag{1.5}$$

and $\tau = \frac{1+\sqrt{5}}{2}$.

The inverse matrices of (1.2) and (1.3) are defined as

$$Q^{-2x} = \begin{pmatrix} cF_s(2x-1) & -sF_s(2x) \\ -sF_s(2x) & cF_s(2x+1) \end{pmatrix}, \tag{1.6}$$

$$Q^{-(2x+1)} = \begin{pmatrix} -sF_s(2x) & cF_s(2x+1) \\ cF_s(2x+1) & -sF_s(2x+2) \end{pmatrix}. \tag{1.7}$$

The basic idea of this cryptosystem is as follows:

1. a plaintext $a_1, a_2, a_3, a_4, \ldots$ is presented in the form of 2×2 matrices

$$M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix},$$

2. then for some $1 \leq i \leq 24$, the permutation π_i of a_1, a_2, a_3, a_4 is designated, i.e, $\pi_i(a_1), \pi_i(a_2), \pi_i(a_3), \pi_i(a_4)$;

3. the matrix (1.2) or (1.3), which is the *enciphering matrix*, and its inverse matrix (1.6) or (1.7) are chosen and named the *deciphering matrix*.

4. the ciphertext $E_1(x)$ or $E_2(x)$ is achieved by applying matrix multiplication of the plaintext M and Q^{2x} or Q^{2x+1}, i.e.,

$$E_1(x) = M \times Q^{2x},$$

   or

$$E_2(x) = M \times Q^{2x+1}.$$

5. To recover the original plaintext M the corresponding inverse matrix Q^{-2x} or Q^{-2x-1} is applied, i.e.,

$$M = E_1(x) \times Q^{-2x},$$

or

$$M = E_2(x) \times Q^{-2x-1}.$$

For more details on the k-Fibonacci hyperbolic functions, the Golden matrices and the Golden cryptography, refer (Stakhov, 2007; Esmaeili and Esmaeili, 2010)

1.3 Problem Statement and Motivation

The principal defect of a symmetrical cryptography such as GC is the key to a transmission problem. The other main issue is the problem of trust between two parties that share a secret symmetric key. The problems of trust may be encountered when the encryption is used for authentication and integrity verification. A symmetric key can be used to verify the identity of other communicating party, but this requires the trust of another party. The most general symmetric cryptosystems are matrix cryptosystems and GC. Any cryptosystem is secure if it is at least resistant to four basic attacks; known-plaintext attack, chosen-plaintext attack, chosen-ciphertext attack and ciphertext-only attack. Ray and Sánchez (Rey and Sánchez, 2008) believed that the GC is not resistant against some of the cryptanalytic attacks. They have proven that the cryptographic method suggested in (Stakhov, 2007) is not secure, i.e., it is not preserved from the chosen-plaintext attack. Also the GC using k-Fibonacci number (KGC) and the GC using Hadamard product (HGC) have the same problem. Specifically, it is shown that the security of such cryptosystems is also compromised as they are not resistant to the basic cryptanalytic attacks: the chosen plaintext attack. These mentioned problems in addition to the beauty and simplicity of the Fibonacci numbers are the motivation to develop and improve the security of GC and using this system is very fast, easy for technical realization, and reliable cryptosystems.

1.4 Objectives

The objectives of this study are as follows:

1. To investigate the insecurity of KGC and HGC.
2. To propose a new extension of golden cryptography based on one-way hash function and discrete logarithm problem (GCHDLP) with an improved security.

3. To compare the security of GCHDLP and the existing golden cryptosystem (GC).

4. To evaluate the GCHDLP and GC by three measuring factors.

1.5 Scope and Limitations of the Work in the Thesis

The scope of this research is outlined as follows:

1. All matrix used in this thesis is 2×2 dimension.

2. All variables are real numbers.

3. The focus of this thesis is mainly on the variants of GC; namely KGC and HGC.

4. The GCHDLP proposed in this work is applied to image encryption.

5. The image size encrypted by GCHDLP is 256×256 pixels.

1.6 Methodology

GC is a symmetric cryptosystem using Fibonacci matrix as the main components to encrypt any string of real number as a secret key used between the sender and the recipient to encrypt and decrypt any plaintext. In this method, it was necessary for both sender and recipient to have the same key. GC, like every symmetric cryptography algorithm, is typically fast and suitable for processing large stream of data which is referred as block ciphers. But the problem of GC is the weakness in security. To solve this problem, mixing the GC with public key algorithms can obtain a combination of security and speed. Unfortunately, the two extensions of GC that presented were still incapable to overcome the infirmity of this system. The first algorithm used k-Fibonacci matrix (KGC) to build an extended version of GC and to increase the security (Stakhov, 2007). The KGC used two secret key, x as the real number and k as the integer number. The second algorithm used Hadamard product (HGC) to make a new system and try to show that this system is more trustworthy than GC (Ernastuti et al., 2010; Nally, 2007). In Chapter 3, both were mathematically proven that they were still friable against basic attacks specially chosen-plaintext attacks. In this thesis, the GCHDLP was proposed which is a cryptosystem made from several materials such as GC, golden matrix, hyperbolic sine and cosine, hash function, and discrete logarithm problem. Then the security of this system was tested against the four basic attacks. This new proposed GCHDLP has made a comparison of secureness with GC against the four basic attacks. Finally, to declare the ability of proposed system, the degree of ability of GC and GCHDLP cipher to hide the pattern of four images are tested. The pictures were: Lena is the reference image and will be used as an example in image processing, Nike and Mickey are the images containing big surface of single color and Damavand (the highest mountain peak in Iran) is a sample with high-frequency. Also both systems were evaluated experimentally by using maximum deviation factor (M1), correlation coefficient factor (M2), and irregular deviation factor (M3).

1.7 Contributions

The contributions of this research are as follows:

1. The variance of golden cryptosystem KGC and HGC were proven to be not secure against chosen plaintext attack.
2. The new extension of original golden cryptosystem using discrete logarithm problem and hash function (GCHDLP) was proposed.
3. The GCHDLP was shown to be resistant to the four above-mentioned basic attacks.
4. By experimental results, it was proven that the proposed GCHDLP provides better encryption quality compared to the encryption of GC.

1.8 Thesis Organization

The structure of this thesis is:

- Chapter 1 is the introduction of whole work done within the scope of the research.
- Chapter 2 is the review of two fundamental concepts in which the next chapters are based on. The part of asymmetric cryptography and symmetric cryptography include stream cipher and block cipher.

- Chapter 3: This chapter is divided into three sections; Section 3.1 introduced the golden cryptography and then the security is investigated, Section 3.2 proves that the generalize golden cryptography by using Hadamard product is still not secure against some types of basic attack, and in Section 3.3 the security of golden cryptosystem using k-Fibonacci number is tackled.

- Chapter 4: In this chapter, by using discrete logarithm problem (DLP) and one-way hash function, a new variant of golden cryptography will be offered. It is a newly proposed version of golden cryptography and more secure than the original GC and the generalized GC (using k- Fibonacci number), also this chapter revealed that the new generalized GC is safe and resistant to the four basic attacks.

- Chapter 5: This chapter presents the new variant of golden cryptography to overcome the disadvantages of golden cryptography. The proposed technique considers different encryption key for each block encryption. Then, computationally and visually, the experiments proved that the suggested variant provides higher encryption quality compared to the original one.

- Chapter 6: This chapter includes conclusions and some open problems.

REFERENCES

Abuturab, M. R. 2014. An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain. *Optics and Lasers in Engineering* 58: 39–47.

Acharya, B., Sharma, M. D., Tiwari, S. and Minz, V. K. 2010. Privacy protection of biometric traits using modified hill cipher with involutory key and robust cryptosystem. *Procedia Computer Science* 2: 242–247.

Ahmad, I. and Shoba Das, A. 2005. Hardware implementation analysis of SHA-256 and SHA-512 algorithms on FPGAs. *Computers & Electrical Engineering* 31 (6): 345–360.

Akbulak, M. and Bozkurt, D. 2009. On the order-m generalized Fibonacci k-numbers. *Chaos, Solitons & Fractals* 42 (3): 1347–1355.

Akhavan, A., Samsudin, A. and Akhshani, A. 2015. Cryptanalysis of an improvement over an image encryption method based on total shuffling. *Optics Communications* 350: 77–82.

Amin, M., Faragallah, O. S. and El-Latif, A. A. A. 2010. A chaotic block cipher algorithm for image cryptosystems. *Communications in Nonlinear Science and Numerical Simulation* 15 (11): 3484–3497.

Bao, L. and Zhou, Y. 2015. Image encryption: Generating visually meaningful encrypted images. *Information Sciences* 324: 197–207.

Barchett, L., Banerji, A., Tracey, J. and Cohn, D. 1996. Problems using MD5 with IPv6. *Performance evaluation* 27: 507–518.

Basin, S. 1963. The appearance of Fibonacci numbers and the Q matrix in electrical network theory. *Mathematics Magazine* 84–97.

Basu, M. and Prasad, B. 2010. Long range variations on the Fibonacci universal code. *Journal of Number Theory* 130 (9): 1925–1931.

Cid, C. 2006. Recent developments in cryptographic hash functions: Security implications and future directions. *Information security technical report* 11 (2): 100–107.

Coppersmith, D., Halevi, S. and Jutla, C. 2002. Cryptanalysis of stream ciphers with linear masking. *Advances in Cryptology CRYPTO 2002* 117–128.

Courtois, N. 2001. The security of hidden field equations (HFE). *Topics in Cryptology CT-RSA 2001* 266–281.

Cusick, T., Ding, C. and Renvall, A. 2004. *Stream ciphers and number theory*. , vol. 66. Elsevier Science.

de Leeuw, K. 2003. The Dutch Invention of the Rotor Machine, 1915–1923. *Cryptologia* 27 (1): 73–94.

Deng, X. 2015. Optical image encryption based on real-valued coding and subtracting with the help of QR code. *Optics Communications* 349: 48–53.

Dey, S. 2012. SD-AREE: A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted. *arXiv preprint arXiv:1205.4279* .

Diffie, W. and Hellman, M. 1976. New directions in cryptography. *Information Theory, IEEE Transactions on* 22 (6): 644–654.

Ding, J. 2004. A new variant of the Matsumoto-Imai cryptosystem through perturbation. *Public Key Cryptography–PKC 2004* 305–318.

Ding, J., Hu, L., Nie, X., Li, J. and Wagner, J. 2007. High order linearization equation (HOLE) attack on multivariate public key cryptosystems. *Public Key Cryptography–PKC 2007* 233–248.

Ding, L., Jin, C. and Guan, J. 2015. Slide attack on standard stream cipher Enocoro-80 in the related-key chosen IV setting. *Pervasive and Mobile Computing* .

Dworkin, M., of Standards, N. I. and (US), T. 2004. *Recommendation for block cipher modes of operation: The CCM mode for authentication and confidentiality*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

El Fishawy, N. F. and Zaid, O. M. A. 2007. Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms. *IJ Network Security* 5 (3): 241–251.

Ernastuti, E., Salim, R. and Sulistyo, S. 2010. THE APPLICATION OF ELC NUMBERS TO GOLDEN CRYPTOGRAPHY (0).

Esmaeili, M. and Esmaeili, M. 2010. A Fibonacci-polynomial based coding method with error detection and correction. *Computers & Mathematics with Applications* 60 (10): 2738–2752.

Falcon, S. and A.Plaza. 2009. k- Fibonacci sequence modulo m. *Chaos, Solitons and fractals* 41: 497–504.

Falcon, S. and Plaza, A. . 2007a. On the Fibonacci K -Number. *Chaos, Solitons and fractals* 32: 1615–24.

Falcon, S. and Plaza, A. 2007b. The k -Fibonacci sequence and the Pascal 2-triangle. *Chaos, Solitons and fractals* 33(1): 38–49.

Falcón, S. and Plaza, A. 2008. The k-Fibonacci hyperbolic functions. *Chaos, Solutions and Fractals* 38: 409–420.

Faugere, J. and Joux, A. 2003. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. *Advances in Cryptology-CRYPTO 2003* 44–60.

FIPS. 2002. “Secure Hash Standard”. *NIST U.S. Department of Commerce* 180-2.

FIPS, P. 2000. 186-2. Digital signature standard (DSS). *National Institute for Standards and Technology* .

Fouque, P., Granboulan, L. and Stern, J. 2005. Differential cryptanalysis for multivariate schemes. *Advances in Cryptology–EUROCRYPT 2005* 577–577.

Freixas, J. and Kurz, S. 2013. The golden number and Fibonacci sequences in the design of voting structures. *European Journal of Operational Research* 226 (2): 246–257.

Golic, J. 1996. Linear models for keystream generators. *Computers, IEEE Transactions on* 45 (1): 41–49.

Goubin, L. and Courtois, N. 2000. Cryptanalysis of the TTM cryptosystem. *Advances in CryptologyASIACRYPT 2000* 44–57.

Gould, H. 1981. A history of the Fibonacci Q-matrix and a higher-dimensional problem. *Fibonacci Quart* 19 (3): 250–257.

Gupta, I., Singh, J. and Chaudhary, R. 2007. Cryptanalysis of an Extension of the Hill Cipher. *Cryptologia* 31 (3): 246–253.

H, M. 1978. Permanents. *In Encyclopaedia of Mathematics and Its Applications* 6.

Hastad, J. 2007. The security of the IAPM and IACBC modes. *Journal of Cryptology* 20 (2): 153–163.

Hoggatt, V. 1969. *Fibonacci and Lucas numbers*. Houghton Mifflin Boston.

Ismail, I., Amin, M. and Diab, H. 2006. How to repair the Hill cipher. *Journal of Zhejiang University SCIENCE A* 7 (12): 2022–2030.

Johnson, D., Menezes, A. and Vanstone, S. 2001. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security* 1 (1): 36–63.

Johnson, R. 2008. *Fibonacci numbers and matrices*.

Kamalakannan, V. and Tamilselvan, S. 2015. Security Enhancement of Text Message Based on Matrix Approach Using Elliptical Curve Cryptosystem. *Procedia Materials Science* 10: 489–496.

Kipnis, A. and Shamir, A. 1999. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in cryptologyCRYPTO99*, 19–30. Springer.

Klein, A. 2008. Attacks on the RC4 stream cipher. *Designs, Codes and Cryptography* 48 (3): 269–286.

Koblitz, N. 1998. *Algebraic aspects of cryptography*. , vol. 3. Springer-Verlag New York Inc.

Kohno, T., Viega, J. and Whiting, D. 2003. The CWC authenticated encryption (associated data) mode. *ePrint Archives* .

Krishna, A. and Madhuravani, K. 2012. A Modified Hill Cipher using Randomized Approach. *International Journal of Computer Network and Information Security (IJCNIS)* 4 (5): 56.

Lima, J. B., Panario, D. and Campello de Souza, R. 2010. Public-key encryption based on Chebyshev polynomials over GF (q). *Information Processing Letters* 111 (2): 51–56.

Lin, C., Lee, C. and Lee, C. 2004. Comments on Saeednia's improved scheme for the Hill cipher. *Journal of the Chinese institute of engineers* 27 (5): 743–746.

Lu, J., Wei, Y., Kim, J. and Pasalic, E. 2014. The higher-order meet-in-the-middle attack and its application to the Camellia block cipher. *Theoretical Computer Science* 527: 102–122.

Menezes, A., Van Oorschot, P. and Vanstone, S. 1997. *Handbook of applied cryptography*. CRC.

Meng, X. and Zheng, X. 2015. Cryptanalysis of RSA with a small parameter revisited. *Information Processing Letters* 115 (11): 858–862.

Mishra, D., Sharma, R., Ranjan, R. and Hanmandlu, M. 2015. Security of RGB image data by affine hill cipher overSL n (F q) and M n (F q) domains with Arnoldtransform. *Optik-International Journal for Light and Electron Optics* .

Moh, T. 1999. A public key system with signature and master key functions. *Communications in Algebra* 27 (5): 2207–2222.

Nally, A. 2007. On the Hadamard product of golden matrices. *Int. J. Contemp. Math Sciences* 2: 537–544.

Nambiar, V. P., Khalil-Hani, M. and Zabidi, M. M. 2009. Accelerating the AES encryption function in OpenSSL for embedded systems. *International Journal of Information and Communication Technology* 2 (1-2): 83–93.

Overbey, J., Traves, W. and Wojdylo, J. 2005. On the keyspace of the Hill cipher. *Cryptologia* 29 (1): 59–72.

Patarin, J. 1995. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt88. *Advances in CryptologyCRYPT095* 248–261.

Patarin, J. 1996. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms 33–48.

Patil, C. G. D. M. B. and Gawali3, B. W. 2010. A review on digital signature schemes. *International Journal of Mathematics, Computer Sciences and Information Technology* 3: 387–402.

Paul, S. 2006. *Cryptanalysis of Stream Ciphers Based on Arrays and Modular Addition*. PhD thesis, Citeseer.

Pfitzmann, A. and Aβmann, R. 1993. More efficient software implementations of (generalized) DES. *Computers & Security* 12 (5): 477–500.

PUB, N. 1977. 46-3. Data Encryption Standard. *Federal Information Processing Standards, National Bureau of Standards, US Department of Commerce* .

Qian, Z., Zhang, X. and Ren, Y. 2015. JPEG encryption for image rescaling in the encrypted domain. *Journal of Visual Communication and Image Representation* 26: 9–13.

Reddy, K. A., Vishnuvardhan, B., Krishna, A. et al. 2012. A Modified Hill Cipher Based on Circulant Matrices. *Procedia Technology* 4: 114–118.

Rey, A. and Sánchez, G. 2008. On the security of the "golden cryptography. *International Jounal of Network Security* 7: 448–450.

Rogaway, P., Bellare, M. and Black, J. 2003. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security (TISSEC)* 6 (3): 365–403.

Saarinen, M.-J. O. 2012. Cycling attacks on GCM, GHASH and other polynomial MACs and hashes. In *Fast Software Encryption*, 216–225. Springer.

Satoh, A. and Inoue, T. 2007. ASIC-hardware-focused comparison for hash functions MD5, RIPEMD-160, and SHS. *Integration, the VLSI Journal* 40 (1): 3–10.

Scheneier, B. 1996. *Applied Cryptography Second Edition: protocols, algorithms, and source code in C*. John Wiley and Sons.

Schneier, B. and Sutherland, P. 1995. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc.

Seberry, J. and Pieprzyk, J. 1989. *Cryptography: an introduction to computer security*. Prentice-Hall, Inc.

Shor, P. 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* 303–332.

Siegenthaler, T. 1985. Decrypting a class of stream ciphers using ciphertext only. *Computers, IEEE Transactions on* 100 (1): 81–85.

Stakhov, A. 1984. Codes of the golden proportion. *Moscow: Radio and communications* .

Stakhov, A. 2003. Hyperbolic Fibonacci and Lucas functions: A new mathematics for the alive nature .

Stakhov, A. 2006. Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the golden cryptography. *Moscow: Academy of Trinitarism* 1138–1146.

Stakhov, A. 2007. The "golden" matrices and a new kind of cryptography. *Chaos, Solutions and Fractals* 32: 1138–1146.

Stakhov, A. and Rozin, B. 2005. On a new class of hyperbolic functions. *Chaos, Solitons & Fractals* 23 (2): 379–389.

Stakhov AP, T. I. 1993. Hyperbolic Fibonacci trigonometry. *Rep Ukr Acad Sci [In Russian]* (7): 914.

Stinson, D. 2006. *Cryptography: theory and practice*. CRC press.

Ugus, O., Huss, I. and Laue, D. 2007. Asymmetric Homomorphic Encryption Transformation for Securing Distributed Data Storage in Wireless Sensor Networks. *Technische Universit" at Darmstadt-in Cooperation with NEC Europe Ltd., Heidelberg, Darmstadt* .

Vasco, M. I. G., del Pozo, A. L. P., Duarte, P. T. and Villar, J. L. 2014. Cryptanalysis of a key exchange scheme based on block matrices. *Information Sciences* 276: 319–331.

Wang, B., Wei, X. and Zhang, Q. 2013. Cryptanalysis of an image cryptosystem based on logistic map. *Optik-International Journal for Light and Electron Optics* 124 (14): 1773–1776.

Wang, L., Yang, B., Hu, Y. and Lai, F. 2006. A medium-field multivariate public-key encryption scheme. *Topics in Cryptology–CT-RSA 2006* 132–149.

Wang, S., Ke, H., Huang, J. and Chan, C. 2007. Concerns about Hash Cracking Aftereffect on Authentication Procedures in Applications of Cyberspace. *Aerospace and Electronic Systems Magazine, IEEE* 22 (1): 3–7.

Wang, X., Luan, D. and Bao, X. 2014. Cryptanalysis of an image encryption algorithm using Chebyshev generator. *Digital Signal Processing* 25: 244–247.

Wang, X., Wang, X., Zhao, J. and Zhang, Z. 2011. Chaotic encryption algorithm based on alternant of stream cipher and block cipher. *Nonlinear Dynamics* 63 (4): 587–597.

Wu, H. 2005. The misuse of RC4 in Microsoft Word and Excel. *Cryptography ePrint Archive* 7: 2005.

Zhang, Y., Xiao, D., Wen, W. and Wong, K.-W. 2014. On the security of symmetric ciphers based on DNA coding. *Information Sciences* 289: 254–261.

Zhou, G., Zhang, D., Liu, Y., Yuan, Y. and Liu, Q. 2015. A novel image encryption algorithm based on chaos and Line map. *Neurocomputing* .