UNIVERSITI PUTRA MALAYSIA

EXTENSION 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
COPYRIGHT

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia
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 sifer dan serangan pilihan teks sifer.

Keputusan eksperimen menggunakan beberapa imej (Lena, Nike, Micky dan Damar-vand) 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 Malaysia, 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 Sharabayan 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 Zulkarnain, 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 responsibilities 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

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ABSTRACT</strong></td>
<td>i</td>
</tr>
<tr>
<td><strong>ABSTRAK</strong></td>
<td>ii</td>
</tr>
<tr>
<td><strong>ACKNOWLEDGEMENTS</strong></td>
<td>iii</td>
</tr>
<tr>
<td><strong>APPROVAL</strong></td>
<td>iv</td>
</tr>
<tr>
<td><strong>DECLARATION</strong></td>
<td>vi</td>
</tr>
<tr>
<td><strong>LIST OF TABLES</strong></td>
<td>xi</td>
</tr>
<tr>
<td><strong>LIST OF FIGURES</strong></td>
<td>xii</td>
</tr>
<tr>
<td><strong>LIST OF ABBREVIATIONS</strong></td>
<td>xii</td>
</tr>
</tbody>
</table>

## CHAPTER

### 1 INTRODUCTION

1.1 Cryptography ........................................ 1
1.2 Golden Cryptography .................................. 4
1.3 Problem Statement and Motivation ................. 6
1.4 Objectives ............................................ 6
1.5 Scope and Limitations of the Work in the Thesis 7
1.6 Methodology .......................................... 7
1.7 Contributions ......................................... 8
1.8 Thesis Organization .................................. 8

### 2 LITERATURE REVIEW

2.1 Introduction .......................................... 10
2.1.1 Definition and Terminology ...................... 10
2.2 Symmetric Cryptosystem ............................ 13
2.2.1 Stream ciphers .................................. 14
2.2.2 Synchronous stream cipher ...................... 16
2.2.3 Block ciphers .................................... 17
2.2.4 Comparing block cipher with stream cipher 19
2.3 Cryptographic Attacks .............................. 20
2.3.1 Cryptographic Attack Methods .................. 20
2.4 Matrix Cryptography ................................ 22
2.4.1 Hill cipher ...................................... 22
2.4.2 Cryptanalysis of Hill cipher .................... 22
2.5 Hash function ........................................ 24
2.6 Fibonacci Matrices .................................. 26
2.6.1 Fibonacci numbers ................................ 27
2.6.2 Ratio of consecutive terms and the golden ratio 28
2.6.3 Hyperbolic Fibonacci function .................. 28
2.6.4 Fibonacci Q-Matrix ................................ 33
2.6.5 Golden matrices .................................. 36
2.7 Determinants of the “Golden” matrices 39
2.8 Summary 39

3 CRYPTANALYSIS OF GOLDEN CRYPTOSYSTEMS 40
  3.1 The Golden Cryptographic Method 40
    3.1.1 Determinants of the “Golden” matrices 43
    3.1.2 Encryption and decryption time 43
    3.1.3 Key Transmission 44
  3.2 The Chosen-plaintext Attacks Against Original Golden Cryptography 44
  3.3 Generalized Golden Cryptography Based on Hadamard Product 46
    3.3.1 Some properties of the $Q^n \circ Q^{-n}$ matrix 46
    3.3.2 Fibonacci Coding/Decoding Method 52
  3.4 The Chosen-Plaintext Attack Against the Cryptographic Method with Hadamard Product of Golden Matrices 54
  3.5 Generalized Golden Cryptography Based on $k$-Fibonacci Numbers 56
    3.5.1 $k$-Fibonacci Numbers 56
    3.5.2 $k$-Fibonacci Q-matrix 56
    3.5.3 Hyperbolic $k$-Fibonacci functions 57
    3.5.4 The Golden matrices 58
    3.5.5 Some properties of the $k$-Fibonacci Q-matrices 58
    3.5.6 Definition of Golden matrices 58
    3.5.7 The inverse “Golden matrix” 59
    3.5.8 The Golden Cryptography Method 61
  3.6 The Chosen-Plaintext Attack Against the Generalized Golden Cryptographic Method Based on $k$-Fibonacci Numbers 63
  3.7 Summary 65

4 THE PROPOSED GCHDLP CRYPTOSYSTEM 66
  4.1 New Variant of Golden Cryptography 66
    4.1.1 Cryptographic Hash Functions 66
    4.1.2 Discrete Logarithm Problem 67
    4.1.3 An Extended Golden Cryptographic Method 68
  4.2 Cryptanalysis of GCHDLP 71
    4.2.1 Chosen-Plaintext Attack Against GCHDLP and GC 71
    4.2.2 Known-Plaintext Attack Against GCHDLP and GC 72
    4.2.3 Chosen-Ciphertext Attack against GCHDLP and GC 75
    4.2.4 Ciphertext-Only Attack Against GCHDLP and GC 78
  4.3 Computational Costs 80
  4.4 Summary 82

5 COMPARISON BETWEEN GC AND GCHDLP 83
  5.1 Quality of Encryption Measuring Factors 83
  5.2 The maximum deviation factor 84
  5.3 The correlation coefficient factor 84
  5.4 The irregular deviation factor 85
  5.5 Experimental Results 88
  5.6 Summary 92
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Cryptographic attack approaches</td>
<td>20</td>
</tr>
<tr>
<td>2.2</td>
<td>Extended Fibonacci numbers</td>
<td>29</td>
</tr>
<tr>
<td>2.3</td>
<td>Fibonacci $Q$-Matrix</td>
<td>35</td>
</tr>
<tr>
<td>2.4</td>
<td>Fibonacci Numbers</td>
<td>36</td>
</tr>
<tr>
<td>3.1</td>
<td>Encryption, Decryption for Golden system</td>
<td>41</td>
</tr>
<tr>
<td>3.2</td>
<td>Encryption, Decryption for Hadamard product system</td>
<td>52</td>
</tr>
<tr>
<td>4.1</td>
<td>Comparison between GC and GCHDLP</td>
<td>80</td>
</tr>
<tr>
<td>4.2</td>
<td>Computational costs of different schemas for encryption and decryption</td>
<td>82</td>
</tr>
<tr>
<td>5.1</td>
<td>The numerical evaluations for encryption quality of the original GC and GCHDLP</td>
<td>91</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Cryptosystem</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>Example of Scytale Cipher</td>
<td>13</td>
</tr>
<tr>
<td>2.3</td>
<td>A common design for symmetric key cryptography</td>
<td>14</td>
</tr>
<tr>
<td>2.4</td>
<td>ECB Mode</td>
<td>18</td>
</tr>
<tr>
<td>2.5</td>
<td>CBC Mode</td>
<td>19</td>
</tr>
<tr>
<td>5.1</td>
<td>Encryption and Decryption by GC</td>
<td>89</td>
</tr>
<tr>
<td>5.2</td>
<td>Encryption and Decryption by GCHDLP</td>
<td>89</td>
</tr>
<tr>
<td>5.3</td>
<td>Encryption and Decryption by GC</td>
<td>89</td>
</tr>
<tr>
<td>5.4</td>
<td>Encryption and Decryption by GCHDLP</td>
<td>89</td>
</tr>
<tr>
<td>5.5</td>
<td>Encryption and Decryption by GC</td>
<td>90</td>
</tr>
<tr>
<td>5.6</td>
<td>Encryption and Decryption by GCHDLP</td>
<td>90</td>
</tr>
<tr>
<td>5.7</td>
<td>Encryption and Decryption by GC</td>
<td>90</td>
</tr>
<tr>
<td>5.8</td>
<td>Encryption and Decryption by GCHDLP</td>
<td>90</td>
</tr>
</tbody>
</table>
**LIST OF ABBREVIATIONS**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher Block Chaining</td>
</tr>
<tr>
<td>CCM</td>
<td>Combined Cipher Machine</td>
</tr>
<tr>
<td>CFB</td>
<td>The Cipher Feedback</td>
</tr>
<tr>
<td>CTR</td>
<td>Counter</td>
</tr>
<tr>
<td>CWC</td>
<td>Carter-Wegman+CTR</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DLP</td>
<td>Discrete Logarithm Problem</td>
</tr>
<tr>
<td>FIPS PUB</td>
<td>Federal Information Processing Standards Publication</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Code Book</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptosystem</td>
</tr>
<tr>
<td>ELC</td>
<td>Extended Lucas Cube</td>
</tr>
<tr>
<td>GC</td>
<td>Golden Cryptography</td>
</tr>
<tr>
<td>GCM</td>
<td>Galois/ Counter Mode</td>
</tr>
<tr>
<td>GCHDLP</td>
<td>Golden Cryptography using Hash Function and Dlp algorithm</td>
</tr>
<tr>
<td>HF</td>
<td>Hash Function</td>
</tr>
<tr>
<td>HFE</td>
<td>Hidden Fields Equations</td>
</tr>
<tr>
<td>HGC</td>
<td>Extension of GC by using Hadamard product</td>
</tr>
<tr>
<td>IAPM</td>
<td>Integrity Aware Parallelizable Mode</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>KGA</td>
<td>Keystream Generation Algorithm</td>
</tr>
<tr>
<td>KGC</td>
<td>Extension of GC by using k-Fibonacci number</td>
</tr>
<tr>
<td>KSA</td>
<td>Key Scheduling Algorithm</td>
</tr>
<tr>
<td>LFR</td>
<td>Linear Feedback Shift Register</td>
</tr>
<tr>
<td>MD4</td>
<td>Message Digest 4</td>
</tr>
<tr>
<td>MFE</td>
<td>Medium Field Equation</td>
</tr>
<tr>
<td>MIC</td>
<td>Message Integrity Code</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OCB</td>
<td>Offset Codebook</td>
</tr>
<tr>
<td>OFB</td>
<td>Output Feedback</td>
</tr>
<tr>
<td>OTP</td>
<td>One Time Pad</td>
</tr>
<tr>
<td>PIN</td>
<td>Personals Identification Number</td>
</tr>
<tr>
<td>PMI</td>
<td>Perturbed Matsumoto-Imai</td>
</tr>
<tr>
<td>PRNG</td>
<td>Pseudo Random Number Generator</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest Shamir and Adleman</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SPN</td>
<td>Substitution-Permutation Network</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TDE</td>
<td>Triple Data Encryption</td>
</tr>
<tr>
<td>TTM</td>
<td>Tame Transformation Methods</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>R-G-B</td>
<td>Red Green Blue</td>
</tr>
</tbody>
</table>
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 (Schneier, 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 (Schneier, 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 (Schneier, 1996)”\(^2\). 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 \(x^{2^4+1}\) 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 multivariate 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 multivariate 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 \( r \ll n \), 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 multivariate 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

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

where \( n = 0, \pm 1, \pm 2, \pm 3, \cdots, F_{n-1}, F_n, F_{n+1} \) 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 are 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

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

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

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

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

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

\[ Q^{-(2x+1)} = \begin{pmatrix} -sF_s(2x) & cF_s(2x + 1) \\ cF_s(2x + 1) & -sF_s(2x + 2) \end{pmatrix}. \]  
(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 \( 2 \times 2 \) 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 \( \pi_i \) 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 $2 \times 2$ 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 $256 \times 256$ 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


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


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 .


