CRYPTANALYSIS OF POLYNOMIAL RECONSTRUCTION PROBLEM-BASED CRYPTOSYSTEMS

By

SITI NABILAH BINTI YUSOF

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

December 2023

IPM 2023 11

DEDICATIONS

To:
My beloved parents,
Rasilah Said, Mak.
Yusof Ahmad, Abah.
…
My family and friends.

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

CRYPTANALYSIS OF POLYNOMIAL RECONSTRUCTION PROBLEM-BASED CRYPTOSYSTEMS

By

SITI NABILAH BINTI YUSOF

December 2023

Chair : Professor Muhammad Rezal bin Kamel Ariffin, PhD
Institute : Mathematical Research

The Polynomial Reconstruction problem (PRP) was introduced as a new hard problem in post-quantum cryptography. Quantum Algorithm Zoo has referred to this problem. The PRP is formulated in a manner comparable to Reed-Solomon error correction codes. A univariate PRP cryptosystem was presented, and the designers utilized Lagrange interpolation in the decryption process. Nonetheless, the univariate PRP cryptosystem was cryptanalyzed entirely, allowing the plaintext message to be retrieved in polynomial time. A modified version of the univariate PRP cryptosystem, known as the bivariate PRP cryptosystem, was proposed. The bivariate PRP cryptosystem employed the Vandermonde method throughout the decryption procedure. According to the creators of the bivariate PRP cryptosystem, increasing the number of variables in a polynomial improves the cryptosystem's security. This research achieved four results, demonstrating that decryption failure can occur in univariate and bivariate PRP cryptosystems. Subsequently, we performed algebraic cryptanalysis on the bivariate PRP cryptosystem to determine whether it is secure against the Indistinguishable under Chosen-Plaintext Attack (IND-CPA) or capable of complete cryptanalysis. In the third finding, we established a condition where users could safely employ the bivariate PRP cryptosystem if the determinant for polynomial $f(\lambda) = 0 \bmod q$. In the final result, we presented an algebraic cryptanalysis of the multivariate PRP cryptosystem, demonstrating that the system can be IND-CPA insecure or fully cryptanalyzed.

Keyword: Polynomial Reconstruction Problem, univariate, bivariate, multivariate, Indistinguishable Chosen-Plaintext Attack

SDG: Goal 9: Industry, Innovation and Infrastructure

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

KRIPTANALISIS TERHADAP SISTEM KRIPTO BERASASKAN MASALAH PEMBINAAN SEMULA POLINOMIAL

Oleh

SITI NABILAH BINTI YUSOF

Disember 2023

Pengerusi : Professor Muhammad Rezal bin Kamel Ariffin, PhD
Institut : Penyelidikan Matematik

Masalah Pembinaan Semula Polinomial (PRP) diperkenalkan sebagai masalah sulit baru di dalam kriptografi pasca kuantum. Masalah ini telah disebutkan di dalam Quantum Algorithm Zoo. PRP mempunyai perumusan yang setara dengan kod pembetulan ralat Reed-Solomon. Sistem kripto PRP univariat telah dicadangkan di mana sistem kripto ini menggunakan interpolasi Lagrange di dalam proses penyahsulitan. Walau bagaimanapun, sistem kripto PRP univariat telah dianalisis sepenuhnya di mana mesej teks asal boleh diperolehi dalam masa polinomial. Seterusnya, sistem kripto PRP bivariat telah dicadangkan di mana sistem kripto ini adalah versi diubah suai daripada sistem kripto PRP univariat. Sistem kripto PRP bivariat ini menggunakan kaedah Vandermonde di dalam proses penyahsulitan. Pereka sistem kripto PRP bivariat mengatakan bahawa dengan menambahkan bilangan pemboleh ubah di dalam polinomial akan meningkatkan tahap keselamatan sistem kripto. Di dalam penyelidikan ini, kami memperoleh empat hasil di mana kami berjaya menunjukkan bahawa kegagalan penyahsulitan boleh berlaku dalam kedua-dua sistem kripto univariat dan bivariat. Selain itu, analisis kriptografi algebra terhadap sistem kripto PRP bivariat di mana kami berjaya menunjukkan sama ada sistem kripto ini tidak selamat secara ketakbolehbezaan terhadap serangan teks asal terpilih (IND-CPA) atau boleh dianalisis sepenuhnya. Untuk hasil yang ketiga, kami menunjukkan satu keadaan di mana pengguna boleh menggunakan sistem kripto PRP bivariat dengan selamat jika mereka mendapat penentu menjadi $f(\lambda) = 0 \bmod q$. Akhir sekali, di dalam hasil yang ke empat, kami mencadangkan satu analisis kriptografi algebra terhadap sistem kripto PRP multivariat dan kami berjaya menunjukkan bahawa sistem ini sama ada tidak selamat secara IND-CPA atau boleh dianalisis sepenuhnya.

Kata kunci: Masalah Pembinaan Semula Polinomial, univariat, bivariat, multivariat, tidak selamat secara ketakbolehbezaan terhadap serangan teks asal terpilih

SDG: Matlamat 9: Industri, Inovasi dan Infrastruktur

ACKNOWLEDGEMENTS

Alhamdulillah. All praises and thankfulness are to Almighty Allah for this opportunity and for giving me the strength and the knowledge I obtain from Him to complete this thesis through all obstacles and difficulties.

Firstly, I would like to express my deepest gratitude to my supervisor, Professor Dr. Muhammad Rezal Kamel Ariffin, who has patiently guided and encouraged me to do this research from the beginning until its completion. I received a lot of new knowledge from him during my Ph.D. journey. I also want to thank my co-supervisors, Dr. Mohamat Aidil and Dr. Faridah Yunos, for their guidance and feedback on my research. Next, thank you to Dr. Terry Lau, Mrs. Nur Raidah Salim, and Mr. Zahari Mahad for all the knowledge related to Mathematical Cryptography that I received. This research was completed successfully with their advice, assistance, and motivation.

My special thanks to my family, *Mak*, Rasilah Said, *Abah*, Yusof Ahmad, my brothers, and sister-in-law, for their support physically, financially, and emotionally throughout my academic journey. I am grateful and blessed to have them during my ups and downs for giving me inspirational thoughts while completing this research. I love you so much. I would also like to say thank you to my friends from school, UiTM, and UPM for their constant encouragement and for always giving me positive strength throughout my Ph.D. study.

My appreciation also goes to the Ministry of Education of Malaysia with Fundamental Research Grant Scheme (FRGS/1/2019/STG06/UPM/02/8) that supports me financially throughout my Ph.D. journey at Universiti Putra Malaysia.

Thank you all from the bottom of my heart.

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:

Muhammad Rezal bin Kamel Ariffin, PhD
Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohamat Aidil bin Mohamat Johari, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Member)

Faridah binti Yunos, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 8 August 2024

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

PRP	Polynomial Reconstruction Problem
PPTA	Probabilistic Polynomial Time Adversary
GCHQ	Government Communications Headquarters
NIST	National Institute of Standards and Technology
IND-CPA	Indistinguishable under Chosen-Plaintext Attack
PK	Public-Key
CT	Ciphertext
AF	Augot and Finiasz
AAK	Ajeena, Almaliky and Kamarulhaili
RSA	Rivest, Shamir and Adleman
AF-SPRP	Augot and Finiasz Solvable Polynomial Reconstruction Problem

CHAPTER 1

INTRODUCTION

1.1 Introduction of Cryptography

Cryptography is a general term used to define the design and analysis of mechanisms based on mathematical methods that give essential security services (Martin, 2012). The word cryptography is from Latin where "*crypt*" means secret and "*graphia*" means writing. This method has been used since the Spartans in ancient Greeks, where they utilized the scytale. Stinson (2005) notes that cryptography aims to allow communication between two people (Alice and Bob) in an insecure channel so that an adversary, Eve, cannot comprehend what is being said. This channel can be a computer network or telephone line.

The communication between Alice and Bob can be secured by using a cryptosystem which is defined as follows:

Definition 1.1 *(Stinson, 2005) A cryptosystem is a five-tuples* $(\mathscr{P},\mathscr{C},\mathscr{K},\mathscr{E},\mathscr{D})$ *which satisfies the following conditions;*

1. $\mathscr{P}$ *is a finite set of possible plaintexts.*

2. $\mathscr{C}$ *is a finite set of possible ciphertexts.*

3. $\mathscr{K}$ *is a finite set of possible keys.*

4. *For each* $K \in \mathscr{K}$*, there is an encryption rule* $e_K \in \mathscr{E}$ *and a corresponding decryption rule* $d_K \in \mathscr{D}$*. Each* $e_K : \mathscr{P} \to \mathscr{C}$ *and* $d_K : \mathscr{C} \to \mathscr{P}$ *are functions such that* $d_K(e_K(x)) = x$ *for every plaintext element* $x \in \mathscr{P}$*.*

The basic terminologies that are used in cryptography is as follows:

i) **Plaintext** is the original message.

ii) **Ciphertext** is the coded message.

iii) **Cipher** is an algorithm for transforming plaintext to ciphertext.

iv) **Key** is an information used in cipher known only to sender or receiver.

v) **Encrypt** is a process of converting plaintext to ciphertext.

vi) **Decrypt** is a process of recovering ciphertext to plaintext.

There are two categories in cryptography which are symmetric-key cryptography and asymmetric-key cryptography. Symmetric-key cryptography is where both sender and recipient share the same key. For asymmetric-key cryptography is also known as Public-Key (PK) cryptography, which involves two keys: the public-key is used in the encryption process, and the private key is used in the decryption process.

1.2 Symmetric-Key Cryptography

The digital data in our computer consists of binary strings. The symmetric-key cryptography algorithm can convert one binary string into another binary string where the process is shown as follows:

1. A sequence of plaintext bits is taken as input.
2. Perform a series of operations on these bits.
3. Output a sequence of bits that produces the ciphertext.

There are two types of symmetric-key cryptography: stream ciphers and block ciphers. Stream ciphers transform plaintext to ciphertext one bit at a time, where the algorithm picks one bit of plaintext, operates a series of operations, and produces one bit of ciphertext (Schneier, 2007). Block ciphers work by taking a block of plaintext bits, processing them through a sequence of operations to produce a block of ciphertext bits. This allows the plaintext to be converted to the ciphertext one block at a time.

1.3 Public-Key Cryptography

In 1969, James Ellis initially discovered the concept of public-key cryptography while working at the British Government Communications Headquarters (GCHQ) (Silverman et al., 2008). His discovery was categorized as confidential material by the British government and released his discovery after his death in 1997. Whitfield Diffie and Martin Hellman published their well-known paper in 1976 entitled “New Directions in Cryptography”, where the paper showed the public-key encryption system concept.

The publication of Diffie-Hellman was significant because it introduced the basic definition and objectives of a new field of mathematics or computer science where the existence of these fields relied on the existing of digital computer. This publication also contributed to the definition of public-key cryptography and its associated components: one-way function and trapdoor information. We provide the mathematical formulation of public-key cryptography where there are spaces of key

$\mathscr{K}$, plaintext $\mathscr{P}$ and ciphertext $\mathscr{C}$. An element of k of the key space $\mathscr{K}$ represents a pair of keys where

$$k = (k_{priv}, k_{pub}).$$

k_{priv} and k_{pub} represent as *private key* and *public key* respectively. There is a corresponding encryption function for each k_{pub} which is

$$e_{k_{pub}} : \mathscr{P} \to \mathscr{C}.$$

Next, the corresponding decryption function for each k_{priv} is

$$d_{k_{priv}} : \mathscr{C} \to \mathscr{P}.$$

If the pair (k_{pub}, k_{priv}) is in the key space $\mathscr{K}$, then

$$d_{k_{priv}}(e_{k_{pub}}(m)) = m, \qquad \forall m \in \mathscr{P}.$$

The definitions of one-way function and trapdoor information are as follows:

Definition 1.2 ***(One-Way Function)****(Menezes et al., 2018) One-way function is a function f from a set X to a set Y if $f(x)$ is "easy" to compute for all $x \in X$ but for "essentially all" elements $y \in Im(f)$ it is "computationally infeasible" to find any $x \in X$ such that $f(x) = y$.*

Definition 1.3 ***(Trapdoor Information)****(Menezes et al., 2018) Trapdoor information is a secret information hidden within an algorithm.*

The application of public-key cryptography is based on trapdoor one-way function which is defined as follows:

Definition 1.4 ***(Trapdoor One-Way Function)****(Menezes et al., 2018) A trapdoor one-way function is a one-way function $f : X \to Y$ with the additional information which is the trapdoor information where it becomes feasible to discover for any given $y \in Im(f)$, an $x \in X$ such that $f(x) = y$.*

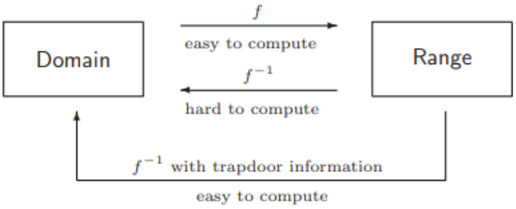

Figure 1.1: Demonstration of one-way function (Hoffstein et al., 2008).

Notice from Figure 1.1, the words ”easy” and ”hard” to compute relies on the time complexity of an algorithm to solve a certain mathematical hard problem. Time complexity and Big-$\mathscr{O}$ notation are defined as follows:

Definition 1.5 ***(Time Complexity)****(Sipser, 2021) Time complexity of an algorithm measures the total of time taken by an algorithm to compute as a function with the length of n string representing the input. The time complexity of an algortihm is usually espressed by using Big-$\mathscr{O}$ notation.*

Definition 1.6 ***(Big-$\mathscr{O}$ Notation)****(Rubinstein-Salzedo, 2018) Given two functions $f(x)$ and $g(x)$, let say that $f(x) = \mathscr{O}g(x)$ if there is some constant $C > 0$, which does not rely on x, hence*

$$|f(x)| \leq Cg(x)$$

for all x.

Remark 1.1 *For all $x \in \mathbb{R}$, however we will use slightly more weakly to mean for all adequately large x, i.e., there exists some H so that $|f(x)| \leq Cg(x)$ for all $x \geq H$.*

From Definition 1.6, as stated by Hoffstein et al. (2008), assume that we wish to solve a mathematical problem where the input can be vary. We want to know how long it takes to solve the problem based on the size of the input. Due to the fact that bits are the unit of measurement for storage required to store an input, they are typically used to determine the size of an input. The following are the definitions describe how to solve a mathematical problem in polynomial time, exponential time, and subexponential time.

Definition 1.7 ***(Polynomial Time)****(Hoffstein et al., 2008) A problem is said to be solvable in polynomial time is when there is a constant $k \geq 0$ where k represents as the input size such that if the input is $\mathscr{O}(n)$ bits long where n represents as the length of the input, then the number of steps to solve the problem is $\mathscr{O}(n^k)$.*

Definition 1.8 ***(Exponential Time)****(Hoffstein et al., 2008) A problem is said to be solvable in exponential time is when there is a constant $c > 0$ such that for input of size $\mathscr{O}(n)$ bits where n represents as the length of the input, then there exists an algorithm that needs $\mathscr{O}(e^{cn})$ steps to solve the problem.*

Definition 1.9 ***(Subexponential Time)****(Hoffstein et al., 2008) A problem is said to be solvable in subexponential time when the number of steps needed to solve the problem for a given input with the size of $\mathscr{O}(n)$ bits is in $\mathscr{O}(e^{\varepsilon n})$ where $0 < \varepsilon < 1$.*

Based on the definitions above, if the mathematical problems are solvable in polynomial time, it is considered "easy". However, if the mathematical problems must be solved in exponential time, then it is considered "hard".

1.4 Post-Quantum Cryptography

Public-key cryptography plays a crucial role in the security of open computer networks, especially the Internet (Buchmann et al., 2017). As public-key cryptography is essential to cyber security, an alternative public-key cryptosystem that is secure from the attack of quantum computers needs to be developed. In 1994, Shor's algorithm was developed, successfully executing the integer factorization and discrete logarithm problems in polynomial time (Shor, 1994). This algorithm proved that the classical cryptographic schemes such as Rivest, Shamir and Adleman (RSA) Cryptosystem and Diffie Hellman Key Exchange Algorithm that depend on such hard mathematical problems would be insecure from the attack of quantum computer.

As mentioned in Alagic et al. (2019), we should be prepared with the adjustment towards post-quantum cryptography as early as ten years from now since we know that the technology keeps on enhancing. Although the replacement for the existing standardized public-key algorithm has yet to be fully ready, we need to focus imperatively on maintaining cryptography agility.

In 2011, a website known as Quantum Algorithm Zoo was created. This website lists many favourable hard mathematical problems considered quantum resistant (Jordan, 2011). The Quantum Algorithm Zoo presented a large-scale catalogue of quantum algorithms which summarize algorithms that can be studied and utilized (Weigold et al., 2021).

The National Institute of Standards and Technology (NIST) called for a quantum-resistant algorithm (Alagic et al., 2019; Song and Zhao, 2017). The chosen public-key cryptosystems will designate one or more algorithms for each digital signature, encryption, and key-establishment. The aim for these algorithms is to protect the sensitive information in the government of United States well into the predictable future, including after the arrival of a quantum computer.

The post-quantum cryptography standardization process is the response from NIST to the evolution of quantum computers. These machines exploit quantum mechanical development to solve hard mathematical problems that are difficult to be solved by conventional computers. If a large-scale quantum computer is built, then the public-key cryptography currently standardized by NIST can be broken. The development of quantum computers will impact the symmetric-key cryptosystem but will not drastically impact it. Post-quantum cryptography aims to create a secure system from the attack of quantum computer (Gaborit et al., 2018).

Nowadays, post-quantum cryptography algorithms are focused on these five approaches which are listed in Table 1.1.

Table 1.1: Post-quantum cryptography algorithms approaches (Ott and Peikert, 2019).

Algorithm	Function	Examples	Characteristics
Hash-based Cryptography	Digital signatures	SPHINCS+, XMSS	Easy to understand reduction of large signature sizes is needed for stateful schemes.
Lattice-based Cryptography	Digital signatures, KEM/Encryption	NTRU, FALCON, NewHope, FrodoKEM, qTESLA	The ciphertext, keys and signatures are short and provides a good perfomance but can be complex.
Code-based Cryptography	KEM/Encryption	HQC, RQC,BIKE	Provides a fast encryption process but the public keys are larger in size.
Multivariate-based Cryptography	Digital signatures	Rainbow, LUOV, EMSS, MQDSS	More analysis is needed for the schemes and the size of key is large.
Supersingular Elliptic Curve Isogeny Cryptography	KEM/Encryption	SIKE	A new approach which uses very small key size but provides slower performance.

1.5 Polynomial Reconstruction Problem (PRP)

In 1999, Polynomial Reconstruction Problem (PRP) was introduced as a new hard problem (Augot and Finiasz, 2003). The PRP is one of the mathematical problems mentioned in Quantum Algorithm Zoo. A public-key cryptosystem based on PRP was presented in Eurocrypt2003 by Augot and Finiasz (Augot et al., 2003; Coron, 2004). The PRP has an equivalent formulation to the Reed-Solomon error correcting codes (Naor and Pinkas, 1999; Sadkhan and Ruma, 2006). The decoding of the Reed-Solomon codes problem is long-established, and many coding theorists were interested when this code was introduced. The goal of decoding is to recover a Reed-Solomon code word from a damaged word, which means a word that contains errors. Decoding Reed-Solomon can be easy if the number of errors is small.

A broad study has been done on the PRP based on its solvability and robustness. From Kiayias and Yung (2004b), the reasons why the PRP is suggested to be a hard mathematical problem because there are some evidences show that PRP can withstand the improvement of quantum computing. Next, this system provides new advantages based on the perspective of efficiency and cost-effectiveness. Lastly, PRP utilizes simple matrix operations and other appealing components that can be useful in cryptographic settings.

The PRP is easy when the weight of error, w, is small such that $w \leq \frac{n-k}{2}$ where n and k represent the number of elements in a vector and the degree of a polynomial, respectively (Augot and Finiasz, 2003). According to Venkatesan Guruswami (1999), this problem has improved to $w \leq n - \sqrt{kn}$. Since Augot and Finiasz created a cryptosystem based on PRP, hence we denoted this system as AF-Cryptosystem. This cryptosystem utilized a univariate polynomial (Kiayias and Yung, 2001, 2004a). The AF-Cryptosystem applied two types of PRP. The first PRP is defined in Jordan (2011), and the second PRP is designed to ensure decryption in which we called the second PRP as the Augot and Finiasz Solvable PRP (AF-SPRP), which is defined as follows:

Definition 1.10 ***(Augot and Finiasz Solvable PRP)*** *(Augot and Finiasz, 2003) Given n, k, t and $(x_i, y_i)_{i=1,\cdots,n}$, output any polynomial p such that $deg(p) < k$ and $p(x_i) = y_i$ for at least t values of i where $t = n - w$ and w is the weight of error.*

According to the Definition 1.10, when t points are given on a Cartesian plane, then output a polynomial that fits all the points on the Cartesian plane. Lagrange interpolation is used in the decryption process.

However, in 2004, Coron fully attacked the AF-Cryptosystem where the plaintext can be obtained in polynomial time (Coron, 2004). Next, a modified version of AF-Cryptosystem was created by Ajeena et al. (2013). This cryptosystem used bivariate polynomial and Vandermonde matrix. We denote this modified cryptosystem as

AAK-Cryptosystem. The designers of AAK-Cryptosystem stated that if the number of variables are increased, then the system's security level is increased.

1.6 Problem statements

According to Jordan (2011), one of the hard mathematical problems that is thought to be quantum resistant is the PRP. A few PRP-based cryptosystems have been developed: Augot and Finiasz (2003)'s univariate PRP and Ajeena et al. (2013)'s bivariate PRP. The Coron (2004) has successfully attacked the univariate PRP. This indicates that applying the AF-Cryptosystem is not safe. Despite increasing the number of variables, this cryptosystem may not be sufficiently secure to be used in post-quantum cryptography. The PRP is a strong contender for a cryptosystem, but cryptographers require knowledge of how to build a reliable and safe cryptosystem on the framework of PRP. The goal of this research is to perform algebraic cryptanalysis on bivariate PRP and make some observations about developing a safe PRP cryptosystem for later use.

1.7 Research Objectives and Methodology

In this subsection, we provide our research objectives. We also state a concise explanation of the methodology used in this research to achieve our research objectives.

1. To investigate the efficiency of decryption process in Polynomial Reconstruction Problem based cryptosystem.
   Methodology: This objective is focused on the decryption process in Augot and Finiasz (2003) and Ajeena et al. (2013) cryptosystems. If W which is the weight of big error vector, E in AF-Cryptosystem and AAK-Cryptosystem are large such that $W > k+1$ and $W > k^2$ respectively, then the decryption failure can occur.

2. To establish an algebraic cryptanalysis upon bivariate Polynomial Reconstruction Problem based cryptosystem.
   Methodology: In this objective, we get the motivation to cryptanalyze bivariate PRP cryptosystem from Coron (2004). The methods that we used are Berlekamp-Welch algorithm and modified Coron cryptanalysis strategy. From here, we obtain two types of result where the system can be fully cryptanalyzed or the system is not indistinguishable chosen plaintext attack (IND-CPA) secure.

3. To outline a secure method in utilizing a bivariate cryptosystem based on the Polynomial Reconstruction Problem.
   Methodology: For this objective, we suggest an alternative way to utilize bivariate PRP cryptosystem in a safe way where the user has to cryptanalyze the system in order to determine whether the system that they used is secure

or not. By using Coron cryptanalysis strategy, the user needs to ensure that the determinant for polynomial $f(\lambda)$ is equal to 0. Hence, the system is safe to be used.

4. To develop an algebraic cryptanalysis for a multivariate cryptosystem based on Polynomial Reconstruction Problems.
   Methodology: To achieve this objective, we created a multivariate PRP cryptosystem based on the AAK-Cryptosystem. The methods that are applied in this analysis are Berlekamp-Welch algorithm and modified Coron cryptanalysis strategy. Thus, despite the increasing the number of variable in a polynomial, the system still can be fully cryptanalyzed or the system is not indistinguishable chosen plaintext attack (IND-CPA) secure.

1.8 Thesis outline

This thesis contains 8 chapters which the contents are shown as follows:

Chapter 1 describes the definition of cryptography and the five approaches of cryptography. This chapter also provides an introduction to post-quantum cryptography and the hard mathematical problem utilized in this research which is PRP. The research objectives and the methodology are also described in this chapter.

Chapter 2 discusses the mathematical background involved in this research, such as Reed-Solomon codes and PRP. This chapter also presents the previous work that utilized PRP which are the univariate and bivariate PRP crytosystems. Moreover, relevant preliminary mathematical concepts involved in this research are also provided.

Chapter 3 introduces the methods that are used in this research which are Lagrange interpolation, Vandermonde method, Berlekamp-Welch algorithm and Indistinguishable under Chosen-Plaintext Attack (IND-CPA) attack. We also provide the cryptanalysis method that had been published by Coron (2004). This cryptanalysis is being our reference for the attack on the bivariate and multivariate PRP cryptosystems.

Chapter 4 provides a proposition where the univariate PRP cryptosystem and bivariate PRP cryptosystem can have a decryption failure. When the big error vector, E, has a weight larger than the number of monomials in a secret polynomial $p(x)$ and $p(x,y)$, then decryption failure can occur in univariate and bivariate PRP cryptosystems. We also provide our numerical illustration for this analysis.

Chapter 5 presents an algebraic cryptanalysis on bivariate PRP cryptosystem. The methodology used in this analysis is the Berlekamp-Welch algorithm and a modified cryptanalysis strategy by Coron (2004). The result shows that we obtain two situations where the system can be fully cryptanalyzed or is not Indistinguishable under Chosen-Plaintext Attack (IND-CPA) secure. We also provide our numerical illustration for this analysis.

Chapter 6 explains a proposition where the user can use the bivariate PRP cryptosystem with a condition. The user needs to use the same method in the bivariate cryptosystem and cryptanalyze their system to determine whether it is secure. By using a modified cryptanalysis strategy by Coron (2004), if the determinant for polynomial $f(\lambda)$ is equal to 0 where $f(\lambda) = 0 \bmod q$, then the system is safe to be used. We also provide our numerical illustration for this analysis.

Chapter 7 proposes an algebraic cryptanalysis on a multivariate PRP cryptosystem. We used the Berlekamp-Welch algorithm and a modified cryptanalysis strategy by Coron (2004). The result shows that the system can be either fully cryptanalyzed or not Indistinguishable under Chosen-Plaintext Attack (IND-CPA) secure. We also provide our numerical illustration for this analysis.

Chapter 8 consists of the summary of this research and the future directions of PRP that can be expanded from this research.

REFERENCES

Abdalla, M., Benhamouda, F., and Pointcheval, D. (2016). Public-key encryption indistinguishable under plaintext-checkable attacks. *IET Information Security*, 10(6):388-303.

Ajeena, R. K., Kamarulhaili, H., and Almaliky, S. B. (2013). Bivariate polynomials public key encryption schemes. *International Journal of Cryptology Research,* 4(1):73-83.

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., and Smith-Tone, D. (2019). *Status report on the first round of the NIST post-quantum cryptography standardization process.* US Department of Commerce, National Institute of Standards and Technology.

Arashiro, T., Zer, L., Corn, P., Pilling, G., Virani, A., Jain, M., Miglani, K., Dash, S., Lin, C., and Khim, J. (2023). *"Lagrange interpolation"*: Brilliant. https://brilliant.org/wiki/lagrange-interpolation/

Augot, D., and Finiasz, M. (2003). A public-key encryption scheme based on the polynomial reconstruction problem. *International Conference on the Theory and Applications of Cryptographic Techniques*, 229-240.

Augot, D., Finiasz, M., and Loidreu, P. (2003). Using the trace operator to repair the polynomial reconstruction problem-based cryptosystem presented at Eurocrypt 2003. *Cryptology ePrint Archive*.

Blackburn, S. R. (1995). The Berlekamp-Welch and Berlekamp-Massey algorithms. *In Proceeding of 1995 IEEE International Symposium on Information Theory*, 409.

Bleichenbacher, D., and Nguyen, P. Q. (2000). Noisy polynomial interpolation and noisy chinese remaindering. *International Conference on the Theory and Applications of Cryptographic Techniques,* 53-69.

Buchmann, J., Lauter, K., and Mosca, M. (2017). Post-quantum cryptography state of art. *IEEE Security and Privacy*, 15(4):12-13.

Carstens, T. V., Ebrahimi, E., Tabia, G. N., and Unruh, D. (2020). On quantum indistinguishability under chosen plaintext attack. *The ANZIAM Journal*, 36(2):107-116.

Childs, A. M., Van Dam, W., Hung, S. H., and Shparlinski, I. E. (2015). Optimal quantum algorithm for polynomial interpolation. *arXiv preprint arXiv:1509.09271*.

Coron, J. -S. (2004). Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem. *International Workshop on Public Key Cryptography*, 14-27.

Fu, A., Zhang, X., Xiong, N., Gao, Y., Wang, H., and Zhang, J. (2020). VFL: A Variable Federated Learning With Privacy-Preserving for Big Data in Industrial IoT. *IEEE Transactions on Industrial Informatics*, 18(5):3316-3326.

Gaborit, P., Otmani, A., and Kalachi, H. T. (2018). Polynomial-time key recovery attack on the Faure-Loidreu scheme based on Gabidulin codes. *Designs, Codes and Cryptography*, 86(7):1391-1403.

Garner, L. E. (1988). *Calculus and analytic geometry.* Dellen Publishing Company.

Higham, N. (2021). *"What is a Vandermonde matrix?"*: Applied mathematics, numerical linear algebra and software. https://nhigham.com/2021/06/15/what-is-a-vandermonde-matrix/.

Hoffstein, J., Pipher, J., and Silverman J. H. (2008). *An introduction to mathematical cryptography*. Springer.

Jordan, S. (2011). *"Quantum algorithm zoo"*: US Department of Commerce, National Institute of Standards and Technology. https://quantumalgorithmzoo.org/.

Kiayias, A., and Yung, M. (2001). Polynomial reconstruction based cryptography. *International Workshop on Selected Areas in Cryptography*, 129-133.

Kiayias, A., and Yung, M. (2004a). Cryptanalyzing the polynomial reconstruction based public-key under optimal parameter choice. *International Conference on the Theory and Application of Cryptology and Information Security,* 401-416.

Kiayias, A., and Yung, M. (2004b). Directions in polynomial reconstruction based cryptography. *IEICE transaction on fundamentals of electronics, communications and computer sciences*, 87(5):978-985.

Laneve, C., Lascu, T. A., and Sordoni, V. (2010). The interval analysis of multilinear expressions. *Electronic Notes in Theoretical Computer Science*, 267(2):43-53.

Loidreau, P. (2005). An Algebraic Attack against Augot-Finiasz Cryptosystem (Doctoral dissertation, INRIA). HAL Open Science.

Martin, K. M. (2012). *Everyday cryptography: Fundamental Principles and Applications.* OUP Oxford.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (2018). *Handbook of applied cryptography.* CRC press.

Naor, M., and Pinkas, B. (1999). Oblivious transfer and polynomial evaluation. *Proceeding of the thirty-first annual ACM symposium on theory of computing*, 245-254.

Ott, D., and Peikert, C. (2019). Identifying research challenges in post-quantum cryptography migration and cryptographic agility. *arXiv preprint arXiv:1909.07353*.

Rubinstein-Salzedo, S. (2018). Big O notation and algorithm efficiency. *Cryptography*, 75-83.

Rudra, A. (2007). *Lecture 27: Berlekamp-Welch algorithm* [Lecture notes]. University at Buffalo.

Sadkhan, S. B., and Ruma, K. (2006). Evaluation of polynomial reconstruction problem by using Lagrange interpolation method. *In 2006 2nd International Conference on Information and Communication Technologies*, 1399-1403.

Schneier, B. (2007*). Applied cryptography: protocols, algorithms and source code in C.* John Wiley and Sons.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceeding 35th annual symposium on foundations of computer science*, 124-134.

Silverman, J. H., Pipher, J., and Hoffstein, J. (2008). *An introduction to mathematical cryptography.* Springer.

Sipser, M. (1996). Introduction to the Theory of Computation. *ACM Sigact News*, 27(1):27-29.

Song, B., and Zhao, Y. (2017). Provably secure identity-based identification and signature schemes from code assumptions. *Plos one*, 12(8): e0182894.

Stinson, D. R. (2005). *Cryptography: theory and practice.* Chapman and Hall/CRC.

Szabados, J. (1990). *Interpolation of functions.* World Scientific.

Venkatesan Guruswami, M. S. (1999). Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6), 1757-1767.

Weigold, M., Barzen, J., Leymann, F., and Vietz, D. (2021). Patterns for hybrid quantum algorithms. *In Symposium and Summer School on Service-Oriented Computing*, 34-51.

Wicker, S. B., and Bhargava, V. K. (1999). *Reed-Solomon codes and their applications.* John Wiley and Sons.

Zhu, S., and Han, Y. (2021). Generative trapdoors for public-key cryptography based on automatic entropy optimization. *China Communications*, 18(8):35-46.