COMP90043

Cryptography and Security

SEMESTER 02 2018

Title: Multivariate Public Key Cryptosystems

Group Number: 12

Lei REN	950214 (LEIR1)
Min XUE	897082 (MXUE2)
WenDong CHEN	931018(WENDONGC1)
ZongLin JIANG	862168(ZONGLINJ)

Lei REN's Reflection

As for presentation part, I am responsible for critical analysis and conclusion part. As known to all, in the recent years, researchers have drawn attention to issues about post quantum cryptosystems. By reading a number of related articles, comparisons among various types of post quantum cryptosystems, like the multivariate public key and hash-based cryptosystem, are mentioned during the presentation. In addition, a comparison between post quantum cryptosystems and widespread modern cryptosystem is elaborated in details with regards to certain aspects, such as key size, efficiency, security and etc.. At the end of the presentation, an idea that both hash-based and multivariate public key cryptosystem have limitations is pointed out. Therefore, further studies are required to make both of these cryptosystems optimized and practical in the future.

As for documentation part, according to the feedback, a narrower scope of this topic became the main focus of the project. That is to say, general aspects of post quantum cryptosystems are replaced by only multivariate public key cryptosystem itself. I am responsible for polishing and formatting the report. Moreover, a conclusion was also rewritten during the process. After spending more time in looking through a variety of research papers and journals, more detailed concepts are shown in the report. For instance, further research directions of multivariate public key cryptosystems are all proposed in the conclusion part.

During the process of writing my report, I came across a series of challenges, like how to paraphrase references, how to write report in the academic way and something like that. However, I was strongly stuck in this topic and gained a further understanding of post quantum cryptosystems, not only concept and significance aspects, but also its advantages, disadvantages and further research aspect. More importantly, I am interested in listing the post quantum cryptosystem into one of my future research directions.

Min XUE's Reflection

In the early stage, I am mainly focusing on data collection about the chosen topic of the post-quantum cryptosystems which is quite abstract and complicated for me. After reading all of those materials collected, I participated in the discussion about determining the specific topic we are going to study and wrote the proposal as well.

Since we decide to choose the topic about both the hash-based and multivariate public key cryptosystems, I mainly focus on studying the MPKC from the perspective of conceptual theory and practical application and collaborate with another teammate. The basic algorithm is explained along with the public key and private key used for encryption and decryption respectively. In addition, two main classifications which include Bipolar system and Hybrid system are shown in detail. I also study about some existing MPKC schemes and choose one named Hidden Field Equation cryptosystem (HFE) to explore and introduce in deeper. In addition, an attack that target on the MPKC is also taken into consideration of which the defending way is discussed for further research.

For the presentation part, I write about some background knowledge and present the basic introduction in the video. According to the comment from the tutor after the presentation, we decide to proceed some adjustment to our topic and make it more specific. Hence, we choose to mainly study about the MPKC and dig it with deeper information. So I read about some relevant literature and add more personal thinking into the report.

Except for all the above, I also responsible for constructing the structure of the report, adding reference either from the lecture or form other literature and adjusting in the final stage for the format of the report.

WenDong CHEN's Reflection

Our topic is post-quantum cryptography. Due to the potential threat of quantum computers, today's cryptosystems cannot resist attack any more. Therefore, it is particularly urgent and important to research post-quantum cryptography. In this project, I am responsible for studying multivariate public key cryptosystem and writing this part. Since MPKC requires some background knowledge of mathematics includes field, multivariate polynomial equations, etc., at the beginning, I learned the basics of mathematics online. After that, I read a lot of literature about MPKC, including its classification, key, encryption and decryption process, etc., summarized them into the article. Like other cryptosystems, MPKC has drawbacks. The primary problem is the security of MPKC. That is to say, under a reasonable assumption (time, computing power, memory), it is necessary to solve the provable security problem (resist quantum attack) of MPKC. The second thing is key size. For MPKC, it's usually about tens of KB, which is much larger than the key of today's cryptosystems. Admittedly, MPKC has a great advantage of high efficiency, which is not available in all cryptosystems today. This advantage enables small devices with limited computing power to be highly confidential. All the content about MPKC above is discussed in more detail in the article.

This assignment has deepened my understanding of cryptography. It not only gave me a more comprehensive understanding of the current cryptosystems I learned in the lecture, but also enrich my knowledge through research on this future field. Everything has two sides. The emergence of quantum computers in the future (if possible) will certainly facilitate people's lives. However, while enjoying the convenience brought by high-speed computing, it also needs to resist the potential danger brought by it. Post-quantum cryptography research still has a long way to go.

ZongLin JIANG's Reflection

In this project, I did many researches on how the quantum computers changes cryptography industry. At the beginning, I was allocated to topic about the hash function. I read some books and papers about the relationship between hash function and quantum computers. Many researchers talked about the contribution of hash function on post-quantum. I found that they all agreed with its security. However, the implementation process made it hard to achieve. Some of them complain that it is not practicable to build a practical hash function since the storage consumed by keys is quite large. I then followed their ideas, finding that they may have various approaches to solve it. They proposed different kinds of methods such as the multiple use of keys and use tree structures to store them. During the process of solving problems, they found many new challenges, and then proposal some new methods to improve it. I tried to catch their ideas and understood their thoughts and found that only when methods are implemented will people found its shortcomings. Many of their ideas are quite creative.

After the presentation we were suggested to focus on one specific topic. Then we choose another topic instead of the hash-based function and I was allocated to write the background part. I read papers about another three anti-quantum methods and tried to understand their history and basic principles. This process helps me a lot, and I just realised different approaches all have their pros and cons. It is quite hard to compare and judge different kinds of functions, and researches are all trying to make best use of their strengths and migrate their problems. This reading process opened my eyes and I got quite a lot benefits in this way.

Abstract

In this information era, an increasing number of people are concerned about issues on information assurance. The modern cryptosystem which is widely used for protecting the security of data and information is facing a severe challenge since the quantum computers are rapidly developed. Some widely used cryptography schemes like RSA and DSA will be attacked by quantum computers, leading to serious damage to the security system. Hence, a new research about defending the quantum computing which is named post-quantum cryptography has attracted much more attention to the public in the recent years. There are mainly four types of classes included in the post-quantum cryptography systems, named Hash-based cryptography, Code-based cryptography, Lattice-based cryptography and Multivariate public key cryptography respectively. One of them will be discussed with the deeper analysis in the report which is the Multivariate Public Key Cryptosystems.

1. Introduction

Cryptography is widely used in all aspects of network and information system security, which guarantees the confidentiality, integrity, availability and other important characteristics of information security. The modern cryptographic systems have always been regarded as secure in the past few decades since many of them are based on a series of difficult mathematical problems, like integer factorization and discrete logarithm [1]. In fact, certain cryptosystems, known to all, only have computational security, which means the time consumed to decrypt ciphertext by brute force is further longer than the time-effectiveness of the information, and the cost of cracking ciphertext is rather higher than the value of encrypted information. Nevertheless, the rapid progress in quantum computing poses a challenge to the existing security schemes. It is a new computing model that lies on the principle of quantum mechanics. With its powerful ability of parallel computing, the limits of existing information technology can be easily broken through. Those referred mathematical problems can be solved with polynomial complexity using a quantum computer [2].

Shor algorithm and Grover algorithm are two types of quantum algorithms that are the most threatening to the modern cryptosystems. Once put into practice, some severe consequences will be brought about:

1. All cryptosystems based on integer factorization and discrete logarithms are not secure. For instance, RSA is the most widely used public key encryption algorithm which assumes that it is computationally infeasible to decompose an integer. However, it is very likely to efficiently factorize the number with Shor's algorithm, provided with a large enough quantum computer.
2. The bit security of block cipher and stream cipher will be significantly decreased.

Compared to classic search algorithms, the Grover quantum algorithm has fast space search efficiency which may result in halving the security of symmetric ciphers.

Encryption Algorithm	Type	Function	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Increase the length of key
SHA-2, SHA-3	N/A	Hash function	Larger output needed
RSA	Public key	Digital signature Key generation	Security loss
ECDSA, ECDH	Public key	Digital signature Key exchange	Security loss
DSA	Public key	Digital signature Key exchange	Security loss

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms [3]

In order to defend against the threat of quantum computing, researchers start to study post-quantum system. Post-quantum cryptography is classified as code based, Lattice based, multivariate and hash based cryptography, which can be distinguished by complex mathematical problems, the key length, digital signatures and etc. [4].

- By using randomization in encryption, code-based cryptography can be protected from quantum computers.
- Lattice-based cryptography is one of the optimized cryptosystems because it is not only with high efficiency, but also uses reasonable short keys.
- Cryptosystems in accordance with multivariate polynomial equations over a finite field are defined as the multivariate cryptography.
- Hash-based cryptography, a cryptographic technique by utilizing the security of hash function, is merely restricted to digital signatures [1].

This report will mainly focus on Multivariate Public Key Cryptosystems(MPKC). Basic algorithms will be explained in terms of encryption and signature, following with some practical schemes introduced respectively.

The evaluation will be conducted from the perspective of the effectiveness, efficiency and degree of security. In addition, different types of attacks which target at decrypting the MPKC scheme are presented and the corresponding strategies for defeating the attack will also be discussed. Moreover, further researches required for the study of MPKC will also be included in the report.

2. Background

The latest development of large-scale quantum computer becomes a threat towards the Public Key infrastructures, which is the most popular cryptosystems nowadays. While scientists have proposed various of encryption methods, their security and efficiency are still being challenged, hence none of them become practical. Despite of the advantage of multi-variate cryptography, many other potential methods are also valuable for discussing, such as code-based cryptography, hash-based cryptography, and lattice-based cryptography. All them has both pros and cons, and it is hard to reach a balance point between the security and efficiency, which limit their acceptance by the industrial.

2.1. Code-based Cryptography

The code-based cryptography uses an error correction code primitively, which makes it one-way available. This code may be reviewed as a mistake by third party and the owner can correct them, so it can be regards as a public key encryption. While there's no a set of practical code-based cryptography due to the size of the codewords, its security makes it valuable,

The appearance of quantum computer cannot challenge its security since one of the most known attack methods, Grover's algorithm, cannot speed-up the current attack methods towards code-based cryptosystems. That is because for the Grover's algorithm, its consecutive call uses the result of the previous computing as the input while the classical memory cannot store all these

result in limited time, which means the Grover's algorithm cannot search this part right away. Meanwhile, the quantum computers are also useless towards the iterative step of Wagner's algorithm, which has the same efficient comparing to Grover's algorithm. What's more, the "divided – and conquer" strategy adapted by code-based cryptography which is used to find the low weight code words to guess the structure also have the same efficient comparing with the Grover's algorithm. All these shows that, for the current attack towards code-based cryptographs, the appearance of quantum computer cannot significantly increase the efficient of it.

2.2 Lattice-based Cryptography

Based on the recent progress such as fully homographic encryption, code obfuscation and attribute-based encryptions carried out using lattice-based cryptography, lattice-based cryptography has gained more and more attractions in the last few years. Meanwhile, for the lattice problems, there doesn't exist any quantum algorithms that can be applied to attack it even in the worst case

The construction of lattice-based cryptographic is based on the presumed hardness of lattice problems, it uses n-dimensional space with a periodic structure, and the most basic one is the shortest vector problem (SVP). The most well-known one is developed by Lenstra, Lenstra and Lovasz in 1982 called LLL algorithms that can be great helpful for many cryptanalsysis. In 1987, Schnorr improved the approximation factors by an enxtension of the LLL algorithms.

The space requirement for solving an exact SVP is impractical, which means polynomial time algorithm that can transfer approximate lattice problems to within polynomial factors. Currenty known methods ins either run in exponential time or get a quite inaccurate result, and that is like NP-hard problems. Hencn, quantum computers doesn't work towards lattice problems.

2.3. Hash-based Cryptography

Hash-based digital signature becomes a candidate to the post-quantum digital signature method since the principle of the hash-based signature is distinguished. The cryptographic hash function makes the hash-based digital signature collision resistance so that people cannot sign two documents with the same signature. The unstructured characteristic of hash function limits the speedup of quantum computers' attack. Different cryptographic hash functions also separate the generated signature scheme from hard algorithmic problems, which makes it available from various of symmetric cryptography.

The Lamport–Diffie one-time signature scheme (LD-OTS) makes hash-based cryptography collision resistance, and that guarantees its security. The Winternitz OTS (W-OTS) makes the signature shorter by summing up the simultaneously multiple uses of one string in the several bits of the message digest. However, both are not available for key's multiple use, and Merkle signature scheme (MSS) solves it. The storage for MSS signature keys will be challenging sometimes, so the deterministic pseudo-random number generator (PRNG) is adapted and only the root needs to be recorded. To increase the efficient of key searching, Merkle signature

scheme that uses tree chaining (CMCC) solves it. It is similar to Merkle trees, but rather than diving the Merkle trees into smaller subtrees, it uses independent Merkle trees. Many researchers found that both the root of the one-time signature in CMSS and the authentication route hardly change, so if the generation of these one-time signatures and the authentication routines can be evenly distributed across each step, the time for the worse signature generation case can be saved. The combination of distributed signature generation and CMSS is called GMSS. In this way, the verification process is successively from one one-time signature to the next one, and only when the root of the signature is verified, will this signature be regarded as the valid one.

3. Theory

Recently, multivariate public key cryptography is getting more and more attention and has become a research hotspot. Its security is based on solving multivariate polynomial equations over a finite field (mostly quadratic polynomials), and it has proven to be an NP-hard problem. Many multivariate public key cryptosystems have been developed so far, such as the Matsumoto-Imai public key cryptosystem and its variants, the Oil-Vinegar public key cryptosystem and its variants, etc.

At present, the research on multivariate public key cryptosystems is still premature so that it need continue researching further. On one side, the high efficiency of MPKC attracts people to design safer and more practical encryption system. On the other hand, MPKC has relatively large key space comparing to the modern public key cryptosystem like RSA. Therefore, the design of MPKC with a small key space is an attractive direction. In addition, the improvement of probabilistic method, the analysis of internal disturbance deformation are also immediate areas of research focus.

3.1. Basic knowledge

3.1.1. Field

The non-empty set k, if two operations are defined in k: addition and multiplication, and the following conditions are met:

(1) k is an Abelian group relates to the addition, and its addition identity is 0.

(2) k is an Abelian group relates to the multiplication excepts 0, and its multiplication identity is 1.

(3) Addition and multiplication have the following distribution law:

$$a(b + c) = ab + ac$$

$$(b + c)a = ba + ca$$

3.1.2. Finite Field

If the field k contains only a finite number of elements, then the field k is a finite field, also known as Galois, where q is the number of elements in field k. The number of elements in a domain is called the order of the finite field. The q-order finite field is usually expressed by GF(q) or Fq.

3.1.3. Prime Field

Let q be a prime number, set k is {0, ..., q - 1}. Addition and multiplication are integer addition and integer multiplication of modulo q, respectively, then k is a prime field.

3.1.4. Frobenius Automorphism

Let k be a q-order finite field, and if there is xq = x for any x ∈ k, then the mapping is called a Frobenius mapping.

3.1.5. Multivariate polynomial equations over finite fields

3.1.5.1. General form of multivariate polynomial equations

Let $x_1, x_2, \dots, x_n$ be n variables on the finite field k (plaintext), then a polynomial of these n variables in the field k is represented by f_i, the degree of f_i is d, and m such polynomials form a polynomial group, expressed as F (ciphertext) [5]. then:

$$\mathrm{F} = (f_1, f_2, \dots, f_m)$$

f_i has the following form:

$$f_i(x_1, \dots, x_n) = \sum a_j \prod x_j, 1 \le i \le m, 1 \le j \le n$$

$y_1, y_2, \dots, y_n$ are elements on the finite field k, and the multivariate polynomial equations are defined as:

$$\begin{cases} y_1 = f_1(x_1, \dots, x_n) \\ y_2 = f_2(x_1, \dots, x_n) \\ \vdots \\ y_m = f_m(x_1, \dots, x_n) \end{cases}$$

3.1.5.2 Quadratic Multivariate Polynomial Equations

When the degree of polynomials d = 2, the multivariate polynomial equations on the finite field k are called quadratic multivariate polynomial equations. The general form is as follows:

$$\begin{cases} y_1 = f_1(x_1, \dots, x_n) = \sum\limits_{1 \le j,k \le n} a_{1,j,k} x_j x_k + \sum\limits_{j=1}^{n} b_{1,j} x_j + c_1 \\ \vdots \\ y_i = f_i(x_1, \dots, x_n) = \sum\limits_{1 \le j,k \le n} a_{i,j,k} x_j x_k + \sum\limits_{j=1}^{n} b_{i,j} x_j + c_i \\ \vdots \\ y_m = f_m(x_1, \dots, x_n) = \sum\limits_{1 \le j,k \le n} a_{m,j,k} x_j x_k + \sum\limits_{j=1}^{n} b_{m,j} x_j + c_m \end{cases}$$

where variables $x_1, \dots, x_n \in k$, function values $y_1, y_2, y_3, \dots, y_m \in k$, $a_{i,j,k}$ are quadratic coefficients, $b_{i,j}$ are primary coefficients, c_i are constants, and $a_{i,j,k}, b_{i,j}, c_i \in k$.

3.2. MQ problem

MQ (Multivariate Quadratic) problem refers to solving the quadratic polynomial equations in the domain k=GF(q) as follows:

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ f_2(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

where f_i are polynomial equations over the field k. It has been proved that MQ problem is a NP-hard problem, even the smallest domain k=GF(2). Therefore, MQ problem has become an important tool for constructing public key cryptosystems on finite fields [6].

3.3. General form of multivariate public key cryptosystem

Multivariate Public Key Cryptosystems (MPKC) has the following general form [7]:
Let k be a finite field, n and m be positive integers, and L1, L2 are randomly selected reversible affine transformations on finite field kn and km, respectively. The mapping F is taken as a easily invertible non-linear mapping from kn to km.

$$Y = (y_1, \dots, y_m) = F'(x_1, \dots, x_n) = L_2 \circ F \circ L_1(x_1, \dots, x_n)$$

where $\circ$ represents the mapping, F' is the mapping from kn to km. It can always be expressed as m and n-ary polynomials over a finite field k, in the form:

$$F'(x_1, \dots, x_n) = (f_1, f_2, \dots, f_m)$$

f_i is an n-ary polynomial over the field k and the highest degree is equal to the degree of F.

- Public key

In multivariate public key cryptosystem, the expression of F' is set to public key, i.e., $f_1, f_2, \dots, f_m$.

- Private key

In general, the private key is two reversible affine transformations L1 and L2 and a mapping F (the structure of F can be made public or confidential).
Since the encryption process uses the public key, anyone can do this.

The decryption process is to calculate the inverse F'^{-1} of F' by the private key, corresponding to the inverse f_i^{-1} of each f_i. Inputting the ciphertexts $y_1, \dots, y_m$ to obtain the plaintext $x_1, \dots, x_n$, that is, for i = 1,...,n

$$x_i = f_i^{-1}(y_1, \dots, y_m)$$

Since the calculation of F'^{-1} requires the private key, the decryption process can only be done by someone with the private key. In general, the simplest nonlinear function, quadratic function, is usually chosen as the central mapping F and the public key polynomial.

3.4. Classification of multivariate public key cryptosystem

3.4.1 Bipolar system

Let k be a finite field, k = GF(q). In a bipolar multivariate public key cryptosystem, the ciphertext is given by the mapping F' from kn to km.

$$F'(x_1, \dots, x_n) = (f_1, f_2, \dots, f_m)$$

Where f_i is a n-ary polynomial of k$[x_1, \dots x_n]$.

The construction of mapping F from kn to km is as follows:

$F(x_1, \dots, x_n) = (f_1', f_2', \dots, f_m')$ ，where $f_i \in k[x_1, \dots, x_n]$

For any equation

$F(x_1, \dots, x_n) = (y_1', \dots, y_m')$ ，

it is easy to be solved. Accordingly, it should be quickly to find the original image $F^{-1}(y_1', \dots, y_m')$ of $(y_1', \dots, y_m')$.

Notice that $F^{-1}(y_1', \dots, y_m')$ only means the original image can be found rather than the mapping F is reversible.

Once such a mapping is found, the encryption process can be represented as a combination of three mappings:

$F' = L_2 \circ F \circ L_1$ ，

Where L1 is a random reversible affine transformation from kn to kn, L2 is a random reversible affine transformation from km to km. L1 is used to hide plaintext while L2 is used to hide the special construction of mapping F.

- Public Key

The public key of bipolar system consists of two parts, one of which is field k and its structure while the other part is F' (m polynomials).

- Private Key

The private key of bipolar system consists of two (maybe three) parts which are reversible affine transformation L1 and L2, and whether the mapping F is the third part of the private key should depend on the situation.

- Encryption

To encrypt a plaintext $X = (x_1, \dots, x_n)$, input the plaintext X to the public key polynomial, calculate $F'(X)$, and get $Y = (y_1, \dots, y_m)$ which is the cyphertext.

- Decryption

To decrypt a cyphertext $Y = (y_1, \dots, y_m)$, solve the polynomial equation
$F'(x_1, \dots, x_n) = Y$.
The solution process can be divided into three steps. First calculate $Y_1 = L_2^{-1}(Y)$ by inputting cyphertext Y to the reverse of affine transformation L2, then calculate $Y_2 = F^{-1}(Y_1)$ by inputting Y1 to the reverse of mapping F, finally, input Y2 to the reverse of affine transformation L1 and get the plaintext $X = (x_1, \dots, x_n)$.
The main idea of bipolar multivariable public key cryptosystem is to shield or mask the mapping F by two reversible transformation L1 and L2. Currently, the majority of multivariate public key cryptosystems are bipolar.

3.4.2 Hybrid system

A hybrid multivariate public key cryptosystem uses a mapping H' from kn+m to kl as its public key, i.e.,
$H'(x_1, \dots, x_n, y_1, \dots, y_m) = (h_1', \dots, h_l')$,
where every h_i' is a polynomial of k$[x_1, \dots, x_n, y_1, \dots, y_m]$. As with the bipolar system, in order to construct such a scheme, it is necessary to find a mapping H: $k^{n+m} \to k^l$ which satisfies the following conditions:
(1) Given $(x_1, \dots, x_n)$, equation H$(x_1, \dots, x_n, y_1, \dots, y_m) = (0, \dots, 0)$ is easy to be solved. In most cases, these are linear equations of $y_1, \dots, y_m$.
(2) Given $(y_1, \dots, y_m)$, equation H$(x_1, \dots, x_n, y_1, \dots, y_m) = (0, \dots, 0)$ is easy to be solved. These are special nonlinear equations.
Once such a mapping is found, H' can be expressed as follows:
$H' = L_3 \circ H \circ (L_1 \times L_2)$,
where the definition of L_1: $k^n \to k^n$ and L_2: $k^m \to k^m$ is the same as bipolar system. L3 is a linear mapping from $k^l \to k^l$.

- Public key

The pubic key of hybrid multivariate public key cryptosystem consists of two parts, one of which is the finite field k and its structure while the other part is mapping H', i.e., $h_1', \dots, h_l'$.

- Private key

The private key of hybrid multivariate public key cryptosystem consists of three (maybe four) parts which are the reversible mapping L1, L2 and L3, and whether the mapping H is the forth part of the private key should depend on the situation.

- Encryption

To encrypt a plaintext $X = (x_1, \dots, x_n)$, input the plaintext X directly to the public key polynomial equations,
$H'(x_1, \dots, x_n, y_1, \dots, y_m) = (0, \dots, 0)$,
solve these equations and get the solution $Y = (y_1, \dots, y_m)$ which is the cyphertext.

- Decryption

To decrypt a cyphertext $Y = (y_1, \dots, y_m)$, first calculate the reverse of L3, bring Y into it and get $Y' = L_3^{-1}(Y) = (y'_1, \dots, y'_m)$, then solve the polynomial equations $H(x'_1, \dots, x'_n, y'_1, \dots, y'_m) = (0, \dots, 0)$ and get $X' = (x'_1, \dots, x'_n)$, finally, input X' to the reverse of L1 and get the plaintext $X = L_1^{-1}(X')$.

The main idea of hybrid multivariate public key cryptosystem is to shield or mask the equation $H(X, Y) = (0, \dots, 0)$ by L1, L2 and L3. As with bipolar system, hiding the structure of H is not required. Currently, hybrid system is less popular than bipolar system.

3.5. Attack method

A famous attack method is Patarin's linearization equation. For a cryptosystem, satisfying the linearization equation means that any legal ciphertext variable y_i and the corresponding plaintext variable x_i satisfy the identity:

$$\sum_{i,j=1}^{n,m} a_{ij} x_i y_j + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{m} c_j y_j + d = 0$$

Starting from the expression of central mapping, seek the linearization equations for plaintext through mathematical analysis. By solving this equation, get a linear relationship with respect to some x_i. By bringing these linear relations into the original public key polynomial, the new public key polynomial with reduced plaintext can be obtained by elimination. Repeating the above steps until no more x_i cannot be eliminated. Finally, Using XL algorithm to solve the remaining variables, and calculate the values of all the variables of plaintext [8].

Similarly, there are other attack methods, such as rank attacks, differential attacks [9].

4. Evaluation

4.1 MPKC Security

Several major attack methods for MPKC have been developed. Although great efforts have been made to analyze the efficiency of various attack methods, we still do not fully understand the potential and limitations of these attack methods. At present, still need a lot of work to research the efficiency of the implementation of various attack methods from both theoretical and practical aspects. Sometimes, the implementation of attack method requires a large amount of storage resources and the failure of deciphering is not due to time constraints but memory exhaustion.

Therefore, in order to apply MPKC in the future, the primary problem is the security of MPKC. That is to say, under a reasonable assumption, it is necessary to solve the provable security problem of MPKC. In addition, we need to further study various attack methods to allow us to construct some reasonable assumptions.

It is not difficult to see that MPKC has great potential. We need more mature and profound mathematical structure and mathematical ideas to perfect MPKC. Currently, we should establish

a systematic approach to design the cryptosystem, which requires the deeper indirect and combined algebraic structures.

4.2 Advantages and disadvantages

The encryption and decryption process of MPKC needs to bring plaintext (ciphertext) into the equations to solve ciphertext (plaintext). Compared to today's public key cryptosystems, such as RSA, it does not require a large amount of computation. Therefore, the advantage of MPKC is high efficiency.

In contrast, MPKC has a big drawback: it requires a fairly large public key (tens of KB). This is not a problem at all for today's computers, but it is a big problem if you need to use MPKC on a small device with limited storage resources. For a device with limited communication capabilities, a public key needs to be transmitted every time and this is also a problem due to the big size of the public key.

One idea for solving the key problem is to use sparse polynomial structure. However, some early research results have been broken. Sparse polynomial structure will bring unexpected weaknesses to MPKC. However, sparse polynomial is a good idea, especially from the perspective of practical application. Future research should try to reduce the key size by choosing a sparse polynomial under the premise of ensuring the security of the cryptosystem.

4.3 Compare

	Security towards quantum attack	Key size	Efficiency
AES	No	Small	Low
RSA	No	Small	Low
MPKC	To be proven	Large	High

In the table, we compared the popular cryptosystems AES and RSA with MPKC from all aspects. As we can see clearly, both AES and RSA have small key size which makes it available for both portable devices and computers to store. However, it is not practical to implement them on the devices which has limited computing ability. This is not a problem for MPKC due to its high efficiency. On the contrary, modern cryptosystems has relatively small key size while MPKC doesn’t which should be improved in the future. At present, the main focus of MPKC is security and we still need more profound mathematical idea to optimize MPKC.

4.4 Application of MPKC

Nowadays, more and more small computing devices came into the picture, such as RFID, wireless sensors, PDAs and so on. Generally, these devices have very limited computing power, battery, and storage capacity. Since the encryption and decryption processes of today's cryptosystems require a large amount of computation, it is difficult to apply them to devices with limited computing capabilities. MPKC is well suited for these products due to its high efficiency. Of course, key size problem of MPKC needs to be further researched and optimized in the future.

5. Conclusion

So far, researches on multivariate public key cryptosystems are still incomplete, so scholars have always been endeavouring to study. For one thing, the high efficiency of multivariate public key cryptosystems is drawn attention by people to design more secure and utilized cryptosystems. For another, although with high efficiency, compared with modern cryptosystems, the large key size would be regarded as a disadvantage. Thus, it is an attractive point for researchers to design multivariate cryptosystems by using schemes with small key sizes. Nevertheless, with the rapid development of multivariate public key cryptosystems, researchers also have to face an increasing number of mathematical problems. That is to say, new mathematical tools and thoughts should be proposed in the coming days. In addition, one of the most effective ways is to use sparse polynomial structures. Many scholars have pointed out this idea, but, unfortunately, a lot of researches were aborted because security cannot be guaranteed. But the spare polynomial structure is still practical only if the security of multivariate public key cryptosystem can be assured. And as long as multivariate public key cryptosystems and algebraic geometry are mutually reinforcing, this multivariate scheme can achieve a burgeoning development. Hence, there is no doubt that putting novel mathematical ideas into practice is of vital importance for the development of multivariate public key cryptosystems.

Furthermore, researches on constructing trapdoor based on multivariate public key scheme, enhancing the speed of cryptographical algorithms, optimizing the probability theory and etc. are all playing essential roles on further development of multivariate public key cryptosystems.

References

[1]S. Gajbhiye, S. Karmakar, M. Sharma, and S. Sharma, "Paradigm shift from classical cryptography to quantum cryptography," *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, 2017.

[2]A. Kuznetsov, A. Kiian, M. Lutsenko, I. Chepurko, and S. Kavun, "Code-based cryptosystems from NIST PQC," *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2018.

[3]"Report on Post-Quantum Cryptography - NIST Page." [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf. [Accessed: 20-Oct-2018].

[4]Z. Liu, K.-K. R. Choo, and J. Grossschadl, "Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 158–162, 2018.

[5]J. Patarin, L. Goubin, "Trapdoor one-way permutations and multivariate polyniomials," *In International Conference on Information Security and Cryptology*, 1997

[6]W. Geiselmann, W. Meier, R. Steinwandt, "An attack on the Isomorphisms of Polynomials problem with one secret," *Cryptology ePrint Archive*, Report 2002/143 (2002). Available: http://eprint.iacr.org/2012/143, 2002

[7]L. Wang, B. Yang, Y. Hu, "A Medium-Field Multicariate Public key Encryption Scheme," CT-RSA2006, LNCS, vol. 3860, pp. 132-149, 2016.

[8] J. Ding, D. Schmidt, "A common defect of the TTM cryptosystem," *In proceedings of the technical track of the ACNS'03, ICISA Press*, pp. 68-78, 2003

[9] J. Ding, D. Schmidt, "The new TTM implementation is not secure," In K. Feng, H. Niederreiter, C. Xing editors, Workshop on Coding Cryptography and Combinatorics, CCC2003 Huangshan (China), *Progress in Computer Science and Applied Logic*, Birkhauser Verlag, pp. 113-128, 2004.