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.

1. Basic knowledge

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:

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.

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.

1.4 Frobenius Automorphism

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

1.5 Multivariate polynomial equations over finite fields

1.5.1 General form of multivariate polynomial equations

Let  be n variables on the finite field k (plaintext), then a polynomial of these n variables in the field k is represented by , the degree of  is d, and m such polynomials form a polynomial group, expressed as F (ciphertext). then:

has the following form:

are elements on the finite field k, and the multivariate polynomial equations are defined as:

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:

where variables , function values ,  are quadratic coefficients, are primary coefficients, are constants, and .

2. MQ problem

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

where 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.

3. General form of multivariate public key cryptosystem

Multivariate Public Key Cryptosystems (MPKC) has the following general form:

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.

where ∘ represents the mapping, 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:

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 is set to public key, i.e., .

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 of by the private key, corresponding to the inverse of each . Inputting the ciphertexts to obtain the plaintext , that is, for i = 1,...,n

Since the calculation of 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.

4. Classification of multivariate public key cryptosystem

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.

Where is a n-ary polynomial of .

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

1. ，where
2. For any equation

，

it is easy to be solved. Accordingly, it should be quickly to find the original image  of .

Notice that 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:

，

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 , input the plaintext X to the public key polynomial, calculate , and get which is the cyphertext.

Decryption

To decrypt a cyphertext , solve the polynomial equation

.

The solution process can be divided into three steps. First calculate by inputting cyphertext Y to the reverse of affine transformation L2, then calculate by inputting Y1 to the reverse of mapping F, finally, input Y2 to the reverse of affine transformation L1 and get the plaintext .

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.

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.,

，

where every is a polynomial of . As with the bipolar system, in order to construct such a scheme, it is necessary to find a mapping H: which satisfies the following conditions:

(1) Given , equation is easy to be solved. In most cases, these are linear equations of .

(2) Given , equation is easy to be solved. These are special nonlinear equations.

Once such a mapping is found, H’ can be expressed as follows:

，

where the definition of and is the same as bipolar system. L3 is a linear mapping from .

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., .

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 , input the plaintext X directly to the public key polynomial equations,

，

solve these equations and get the solution which is the cyphertext.

Decryption

To decrypt a cyphertext , first calculate the reverse of L3, bring Y into it and get , then solve the polynomial equations and get , finally, input X’ to the reverse of L1 and get the plaintext .

The main idea of hybrid multivariate public key cryptosystem is to shield or mask the equation 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.

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 and the corresponding plaintext variable satisfy the identity:

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 . 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 cannot be eliminated. Finally, Using XL algorithm to solve the remaining variables, and calculate the values of all the variables of plaintext.

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

6. Evaluation

6.1 MPKC Security

Several major attack methods for MPKC have been developed. They are roughly divided into the following two categories:

Structure-based attack: This attack relies on the specific structure of the corresponding MPKC.

General Attack: This attack uses the general method of solving multivariate polynomial equations.

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.

6.2 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.

6.3 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.

6.4 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.

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.