在最近十几年中，多变量公钥密码收到越来越多的关注，已经成为了研究的热点。它的安全性基础是求解有限域上的多元多项式方程组，大多是二次多项式，而这一问题已经被证明是NP-困难问题。迄今为止已经构造出了许多的多变量公钥密码体制，例如Matsumoto-Imai公钥密码体制及其变体，Oil-Vinegar公钥密码体制及其变体等等。

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.

目前，对多变量公钥系统的研究还远远不够成熟，大量的科研工作者正在投入努力。一方面，多变量公钥的高效率一直吸引着人们去设计更安全和更实用的加密体制。另一方面，虽然多变量共要密码体制的效率较高，但相比于传统的公钥密码体制，多变量公钥具有密钥量较大的缺点。因此密钥量较小的多变量体制的设计也是一个具有吸引力的方向。此外，对多变量公钥密码系统的研究热点还体现在对概率化方法的改进、对内部扰动变形的分析等等。

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. 基础知识
   1. 域

非空元素集合k，若在k中定义了两种运算：加法和乘法，并且满足下述条件：

1. k关于加法构成Abel群，其加法恒等元记为0，
2. k中除零元素外全体对乘法构成Abel群，其乘法恒等元记为1。
3. 加法和乘法有如下分配率：

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. 有限域

若域k中只含有有限个元素，则成该域k为有限域，亦称Galois。其中q为域中元素个数。域中元素的个数称为有限域的阶。q阶有限域，常用GF(q)或Fq表示。

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. 素域

设q是一个素数，集合k为{0,…,q - 1}，加法和乘法运算分别为取模q的整数加法和整数乘法运算，则称k为一个素域。

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. Frobenius自同构

设k是q阶有限域，则对任意的  有xq = x，则称该映射为Frobenius映射。

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. 有限域上多元多项式方程组
     1. 多元多项式方程组的一般形式

设x1, x2, …, xn 是有限域k上的n个变量（代表明文），那么在域k上关于n个变量的某个多项式用fi表示，次数为d，m个这样的多项式构成一个多项式组，用F来表示。则：

F = (f1, f2, …, fm)（代表密文）

其中所有的fi，形式如下：

则y1,y2,…,yn是有限域k上的元素，定义多变量多项式方程组形式为：

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. 二次多变量多项式方程组

当多项式的次数d=2时，有限域k上的多元多变量多项式方程组被称为二次多变量多项式方程组，一般形式如下：

其中变量，函数值，为二次项系数，为一次项系数，为常数，且。

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 .

1. MQ问题

MQ问题指的是求解如下在域中的二次多项式方程组：

其中fi为域k上的多项式方程。经证明MQ问题是NP困难问题，即使是最小的域也不例外。因此MQ问题成为了构造有限域上公钥密码体制的重要工具。

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.

1. 多变量公钥密码系统的一般形式

多变量公钥密码系统 (Multivariate Public Key Cryptosystems, MPKC)具有如下一般形式：

令k是一个有限域，n和m是正整数，L1和L2分别是kn和km上随机选取的可逆放射变换。取映射F为一个从kn和km的容易求逆的非线性映射。令

其中表示映射的合成，是一个从kn到km的映射。它总可以被表示成有限域k上m和n元多项式，形式如下：

为域k上的n元多项式，其最高次数等于F的次数。

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.

公钥

在多变量公钥密码系统中，的表达式设为公钥，即。

私钥

一般情况下，私钥为两个可逆仿射变换L1和L2及映射F。F的结构可以公开，也可以保密。

由于加密过程采用的是公钥，那么任何人均可完成此过程。

解密过程是通过私钥计算的逆，对应于每一个的逆，输入密文，得到明文，即对于i = 1,…,n 有

由于计算需要得知私钥，所以解密过程只能有拥有私钥的人来完成。一般地，中心映射F和公钥多项式通常选取为最简单的非线性函数---二次函数。

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.

1. 多变量公钥密码系统的分类

4.1 双极系统（Bipolar Systems）

令k是一个有限域，k = GF(q)，在一个双极多变量公钥系统中，密文由从kn到km的映射给出，

其中是k[x1,…,xn]中的n元多项式

4. Classification of MPKC

4.1 Bipolar systems

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 .

从kn到km的映射F的构造过程如下：

1. ，其中
2. 对于任意的等式

，

可以很容易的解决。相应的，能够快速的找到唯一的原象。

这里需要注意的是，仅仅意味着能够找到原象，而不是说映射F是可逆的。

一旦找到这样的一个映射，那么加密过程就可以表示成由三个映射合成的组合映射：

，

其中L1是一个随机选定的从kn到kn的可逆仿射变换，L2则是一个随机选定的从km到km的可逆仿射变换。放射变换L1用来隐藏明文变量，L2用来隐藏中心映射F的特殊结构。

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:

，

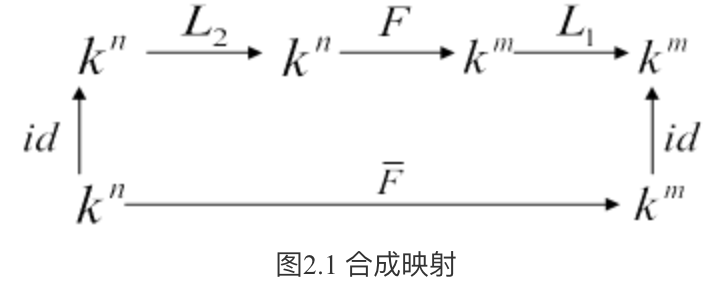
Where L1 is a random reversible affine transformation from kn to kn, L2 is a random reversible affine transformation from km to km. L1 is used to hide plaintext while L2 is used to hide the special construction of mapping F.

公钥

双极系统的公钥包括两个部分，其一是域k及其域结构；其二是的m个多项式。

私钥

私钥包括L1和L2，映射F是否为私钥的一部分可是具体情况而定。



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.

加密过程

若要加密明文消息，我们仅需要将其带入公钥多项式，计算，得到即为加密后的密文。

解密过程

若要解密一个密文消息，则需要求解方程

，

对于该方程的求解，可以先通过求，然后计算，再计算就可以得到对应的明文

验证过程

任何人只要将签名带入等式看是否相等即可验证。

双极多变量系统的主要思想是引入可逆映射L1和L2达到“隐藏”或者“掩盖”映射F的目的，否则映射F的求逆过程将会变得很容易。当前，大多数多变量公钥密码系统都是双极型的。

Encryption

To encrypt a plaintext , input the plaintext X into 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 混合系统

一个混合型多变量公钥方案使用从到的映射作为它的公钥，即

，

其中每一个均为中的多项式。与双极系统一样，为了构建这样的一个方案，需要找到映射H: ，即

其中每一个均为中的多项式，并满足以下条件：

1. 对于任意给定的，方程组

，

很容易求解。在多数情况下，这是一个关于变量的线性方程组

1. 对于任意给定的，方程组

，

很容易求解。这是一组特别设计的非线性方程组。

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, it is linear equations of .

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

一旦找到这样的映射，可以表示为如下的形式：

，

其中和的定义与双极系统中的定义相同。是一个从的线性映射。

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 .

公钥

混合多变量公钥系统的公钥包括两部分：其一是有限域k及其域结构；其二是映射的l个多项式，即。

私钥

私钥部分包括线性可逆映射和线性映射。方程根据不同的情况，可以是密钥的一部分也可以是公钥的一部分。

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.

加密过程

如果要加密明文消息，可直接将其带入

，

得到解，这个Y就是相应的密文。

解密过程

若要解密密文消息，应先计算，得到，再求解方程

，

得到方程的解，明文就由产生。

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 .

混合多变量公钥密码系统的主要思想使用三个映射和来隐藏方程，否则在给定Y的情况下此方程的求解将变得非常容易。与双极系统一样，隐藏H结构形式并不是必须的。目前，混合系统的使用相对较少。

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.

1. 攻击方法

比较著名的攻击方式是Patarin的线性化方程。对于一个密码体制，满足线性化方程式指任意合法的密文变量和相应的明文变量满足恒等式：

从中心映射的表达式出发，通过数学分析，寻求关于明文的线性化方程。通过求解该方程，得到关于某些的线性关系。将这些线性关系带入原公钥多项式，通过消元，即可得到新的约减了的明文分量的公钥多项式，重复上述步骤直到不能消元为止。最后利用XL宣发求解余下变量的值，将这些值代入消元所使用的线性表达式中，并计算出明文所有变量的值，即可恢复原明文。

类似的，还有其他攻击方法，如利用XL算法求解非线性方程，秩攻击，差分攻击等等。

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.

1. Evaluation
   1. MPKC的安全性

目前已经研究出来了几种MPKC的主要攻击方法。它们大致分为以下两类：

基于结构的攻击：这种攻击依赖于相应MPKC的特定结构。

一般的攻击：这种攻击使用求解多变量多项式方程组的一般方法。

尽管已经做了很大的努力来分析各种不同攻击方法的效率，但是我们仍旧没有完全理解一些攻击方法的潜力和局限性。仍旧需要大量的工作从理论和实际两个方面来理解各种攻击方法的实现效率。有的时候，攻击程序实现需要大量的存储资源，运行失败并不是因为时间的限制而是因为内存耗尽。

所以要想在未来实际应用MPKC，首要问题就是MPKC的安全性，也就是说，在一个合理的假设前提下，需要解决MPKC的可证明安全问题。另外，我们也需要进一步研究各种不同的攻击方式，这样才能允许我们构建一些合理假设。

不难看出，MPKC具有巨大的潜力，我们需要更为成熟深奥的数学结构和数学思想来完善MPKC。目前，我们应该建立一个系统化的方法来完成构造密码系统的设计工作，这需要使用来自于代数几何的更深刻的间接和组合代数结构。

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.

* 1. 优点和缺点

MPKC的加密解密过程需要将明文（密文）带入方程组来求解密文（明文）。相比于现如今的公钥密码方案，如RSA，它不需要很大的计算量（超大数量级的乘方运算）。所以MPKC的优点就是在保证安全性能的前提下，具有高效率。

反观MPKC有一个很大的缺点就是它需要一个相当大的公钥（几十KB）。对于现如今的计算机来说，这根本不是一个问题，但是如果需要在存储资源受限的小设备上使用该密码系统，就是一个很大的问题。对于通信能力受限的设备每执行一次都需要传送一个公钥，由于公钥的大小，这也会是一个问题。

对于密钥问题的解决，一种想法就是利用稀疏多项式结构。但是，一些早期的研究结果已经被攻破，它的使用会给MPKC带来意想不到的弱点。然而，稀疏多项式的思想是一个好主意，特别是从实际应用的角度看。未来的研究应在保证密码系统安全性的前提下，尽量选择稀疏多项式来缩减密钥大小。

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.

* 1. MPKC的应用

目前，一些小型的计算设备频繁出现在我们的生活当中，如RFID，无线传感器，PDA等等。这些设备通常仅有非常有限的计算能力，电池，存储容量。由于现如今的私钥密码系统和公钥密码系统的加密解密过程均需要大量的运算，将其运用在这些计算能力有限的设备上是很困难的。MPKC由于其高效率，很适合应用在这些产品上。当然，MPKC的密钥大小问题需要在未来进一步研究并优化。

6.3 Application of MPKC

At present, 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.

可以写在conclusion中：

多变量公钥密码系统(MPKC)的缺点：密钥比传统的公钥密码如RSA或ECC大得多。

MPKC的研究发展提出了新的数学挑战，需要新的数学工具和思想。未来发展中我们希望看到MPKC和代数几何之间的相互促进作用能快速增长。毫无疑问，新数学工具和数学见解的出现，对MPKC的未来发展是至关重要的。

我们将论文主要研究的哈希方法，MPKC与当今典型的公钥密码系统(DES)和私钥密码系统(RSA)进行了对比，结果如下：

表格

从表格中我们可以明确的看出，哈希方法最大的优点就是它的安全性，它能够抵御量子攻击；MPKC最大的优点是它的高效性。虽然这些密码系统都可以应用在如今的计算机上，但对于计算能力受限的设备，MPKC可以应用在其上。

对于密钥大小，我们可以明确的看到这两个后量子密码系统都具有很大的密钥。RSA密钥大小为1Kb左右，DES更小。而MPKC的密钥大小为几十KB，哈希方法的密钥空间甚至更大。根据目前的研究结果，针对哈希方法，我们可以用xxx算法对其进行优化。针对MPKC，我们可以利用稀疏多项式思想进行优化。

对于哈希方法，安全性已经得到了保证，我们需要对其算法效率和密钥大小进行性能优化。对于MPKC，急需解决的是其可证明安全问题，我们需要先完全保证它的安全性，再对其性能进行优化。