Multivariate Public Key Cryptography

Jintai Ding

University of Cincinnati
Technical University of Darmstadt

1. General Introduction
2. Multivariate public key cryptosystems
3. Challenges

1 General Introduction

In June 2006, in Belgium, there was a very successful international workshop on **Post-quantum cryptography** – public key cryptosystems that potentially could resist the future quantum computer attacks.

Currently there are 4 main families:

1) Code-based public key cryptography

2) Hash-based public key cryptography

3) Lattice-based public key cryptography

4) Multivariate Public Key Cryptography

The view from the history of algebra (Diffie)

RSA – Number Theory – the 18th century mathematics

ECC – Theory of Elliptic Curves – the 19th century mathematics

Multivariate Public key cryptosystem – Algebraic Geometry – the 20th century mathematics

Algebraic Geometry – Theory of Polynomial Rings

1.1 Multivariate Public Key Cryptosystems

- *Cryptosystems based on multivariate functions over a finite field instead of single variable functions.*

- The cipher –**the public key** is given as:

$$G(x_1, ..., x_n) = (G_1(x_1, ..., x_n), ..., G_m(x_1, ..., x_n)).$$

Here the G_i are multivariate polynomials over a small finite field k . G can be viewed as a map:

$$G : Onk^n \longrightarrow k^m$$

Encryption

- Any plaintext $M = (x'_1, ..., x'_n)$ has the ciphertext:

$$G(M) = G(x'_1, ..., x'_n) = (y'_1, ..., y'_n).$$

Encryption: Evaluation of the values of the set of polynomials at a point.

Decryption

- To decrypt the ciphertext $(y'_1, ..., y'_n)$, we need to know the hidden structure of G– **the secret key**, so that one can invert the map G to find the plaintext $(x'_1, ..., x'_n)$.

  Decryption relies on the hidden structure of the public key

Multivariate Signature schemes

- To verify, check indeed if the signature and the hash value of the plaintext satisfies the equations given by the public key.

  Document $(y'_1, ..., y'_m)$, signature $(x'_1, ..., x'_n)$, public key $G(x_1, .., x_n)$, $m \leq n$. .

  To verify, we need ro check:

  $$G(x'_1, ..., x'_n) \overset{?}{=} (y'_1, .., y'_m).$$

- To sign, one need to find one solution of the equation above, or to invert the map G.

A Toy Example:

- We use the finite field $k = GF[2]/(x^2 + x + 1)$ with 2^2 elements.
- We denote the elements of the field by the set $\{\mathit{0}, \mathit{1}, \mathit{2}, \mathit{3}\}$ to simplify the notation.

  Here $\mathit{0}$ represent the 0 in k, $\mathit{1}$ for 1, $\mathit{2}$ for x, and $\mathit{3}$ for $1 + x$. In this case, $\mathit{1} + \mathit{3} = \mathit{2}$ and $\mathit{2} * \mathit{3} = \mathit{1}$.

- The public key:

$$
\begin{aligned}
G_0(x_1, x_2, x_3) &= \quad 1 + x_2 + 2x_0x_2 + 3x_1^2 + 3x_1x_2 + x_2^2 \\
G_1(x_1, x_2, x_3) &= \quad 1 + 3x_0 + 2x_1 + x_2 + x_0^2 + x_0x_1 + 3x_0x_2 + x_1^2 \\
G_2(x_1, x_2, x_3) &= \quad 3x_2 + x_0^2 + 3x_1^2 + x_1x_2 + 3x_2^2
\end{aligned}
$$

- For example, if the plaintext is: $x_0 = 1$, $x_1 = 2$, $x_2 = 3$, then we can plug into G_1, G_2 and G_3 to get the ciphertext $y_0 = 0$, $y_1 = 0$, $y_2 = 1$.
- This is a bijective map and we can invert it easily.
- This is an example based on the Matsumoto-Imai cryptosystem.

Direct attack is to solve the set of polynomial equations:

$$G(x_1, ..., x_n) = (y'_1, ..., y'_m)$$

or

$$(G_1(x_1, ..., x_n), ..., G_m(x_1, ..., x_n)) = (y'_1, ..., y'_m),$$

because G and $(y'_1, ..., y'_m)$ are known.

- **Security Foundation**.

  - *Solving a set of n randomly chosen equations (nonlinear) with n variables is NP-complete.*

- **Quadratic Constructions.**

1) Efficiency considerations of key size and computation efficiency lead to mainly quadratic constructions.

$$G_l(x_1, ..x_n) = \sum_{i,j} \alpha_{lij} x_i x_j + \sum_i \beta_{li} x_i + \gamma_l.$$

2) Mathematical structure consideration: any set of high degree polynomial equations can be reduced to a set of quadratic equations.

$$x_1 x_2 x_3 = 1,$$

is equivalent to

$$\begin{aligned} x_1 x_2 - y &= 0 \\ y x_3 &= 1. \end{aligned}$$

- **The Potentials.**

  I.) We have not yet seen how a quantum computer can be used to attack MPKCs efficiently.

  II.) We have seen the potential to build much more efficient public key cryptosystems.

- **MPKCs**

- Early works.

- Matsumoto-Imai.

- HFE and HFEv.

- Oil & Vinegar.

- Sflash (Matsumoto-Imai-Minus) systems, accepted by NESSIE as a security standard for low cost smart cards.

-Quartz, HFEv-Minus: NESSIE

-Rainbow; TTS, TRMC

-Internal Perturbation

- MFE

- TTM systems.

Some Names: Diffie, Fell, Stern, Coppersmith, Tsujii, Shamir, Matsumoto, Imai, Patarin, Goubin, Courtois, Kipnis, Moh, Faugere, Ding, Schmidt, Chen, Yang, Wang, Gilbert, Perret, Sugita, Wolf, ...

2 Multivariate public key cryptosystems

The initial works by Diffie, Fell, Tsujii, Shamir etc were not very successful.

2.1 The Matsumoto-Imai Cryptosystems

2.1.1 Notation

- k is a small finite field of characteristic 2 with $|k| = q$.
- $\bar{K} = k[x]/(g(x))$, a degree n extension of k.
- The standard k-linear invertible map $\phi : \bar{K} \longrightarrow k^n$, and $\phi^{-1} : k^n \longrightarrow \bar{K}$.

  The idea of "Big Field".

  We build maps over $\bar{K}$, then lift it to be a map over k^n.

2.1.2 The MI System

- Proposed in 1988.
- The map F over $\bar{K}$:

$$F : \bar{K} \longmapsto \bar{K},$$
$$F(X) = X^{q^\theta+1}.$$

- Let $\tilde{F}(x_1, \ldots, x_n) = \phi \circ F \circ \phi^{-1}(x_1, \ldots, x_n) = (\tilde{F}_1, \ldots, \tilde{F}_n)$. The $\tilde{F}_i = \tilde{F}_i(x_1, \ldots, x_n)$ are quadratic polynomials in n variables. Why quadratic?

$$X^{q^\theta+1} = X^{q^\theta} \times X.$$

- The cipher $\bar{F}$ is a quadratic multivariate map over k^n:

  $$\bar{F} = L_1 \circ \phi \circ F \circ \phi^{-1} \circ L_2,$$

  where the L_i are randomly chosen invertible affine maps over k^n

  Composition and decomposition of maps.

- The L_i are used to “hide” $\bar{F}$.

- The condition: $\gcd\left(q^\theta + 1, q^n - 1\right) = 1$, ensures the invertibility of the map for purposes of decryption.

  It requires that k must be of characteristic 2.

- $F^{-1}(X) = X^t$ such that:

$$t \times (q^\theta + 1) \equiv 1 \pmod{q^n - 1}.$$

- The public key includes the field structure of k, θ and $\bar{F} = (\bar{F}_1, .., \bar{F}_n)$.
- The secret keys are L_1 and L_2.
- To decrypt, we only have to invert the maps one by one.
- The toy example is produced by setting $n = 3$ and $\theta = 2$.

2.1.3 Attack on MI

- Linearization equation method by Patarin 1995.
- The basic idea is to use the linearization equations (LEs) satisfied by the MI system:

$$\sum a_{ij}x_iy_j + \sum b_ix_i + \sum c_iy_j + d = 0,$$

where $(x_1, ..., x_n)$ is the plaintext and $(y_1, ..., y_n)$ the ciphertext.

$$Y = X^{q^\theta + 1},$$

$$Y^{q^\theta - 1} = X^{q^{2\theta} - 1},$$

$$Y^{q^\theta} X = Y X^{q^{2\theta}},$$

$$Y^{q^\theta} X = Y X^{q^{2\theta}},$$

$$Y^{q^\theta} X - Y X^{q^{2\theta}} = 0.$$

This implies over the small field k, we have equations like

$$\sum a'_{ij} x_i y_j = 0,$$

- There are enough LEs to produce a substantial number of linearly independent linear equations satisfied by the plaintext for any given ciphertext.
- The dimension of linear equations for any given ciphertext (except one case) is $n - GCD(n, \theta)$.

The MI cryptosystem is the catalyst for the recent fast development of the field MKPCs.

2.2 The generalization and extension of MI

Patarin's group.

1.) Direct generalization – MI-Plus – Sflash.

- **Minus**

$$\bar{F}(x_1, ..., x_n) = (\bar{F}_1, ..., \bar{F}_n)$$

$$\bar{F}^{-}(x_1, ..., x_n) = (\bar{F}_1, ..., \bar{F}_{n-r})$$

It is map $k^n - > k^{n-r}$.

- Minus is used to build signature schemes.

- Sflash is a signature scheme, which was accepted as a security standard for low cost smartcards by the Information Society Technologies (IST) Programme of the European Commission for the New European Schemes for Signatures, Integrity, and Encryption project (NESSIE) in 2004.
- Sflash is Matsumoto-Imai-Minus, where one takes out a few components from the public key of a MI system.
- The length of a signature is 249-bits and is much faster than RSA.

- To sign, we find one solution of the equations:

$$\bar{F}^{-}(x_1, ..., x_n) = (\bar{F}_1, ..., \bar{F}_{n-r}) = (y'_1, ..., y'_{n-r}),$$

by putting back the “lost equations”:

$$\bar{F}(x_1, ..., x_n) = (\bar{F}_1, ..., \bar{F}_n) = (y'_1, ..., y'_{n-r}, a_1, ..., a_r),$$

where a_i are randomly chosen.

- **Plus**

$$\bar{F}(x_1, ..., x_n) = (\bar{F}_1, ..., \bar{F}_n)$$

$$\bar{F}^+(x_1, ..., x_n) = \bar{L} \circ (\bar{F}_1, ..., \bar{F}_n, P_1, ..., P_a).$$

- **Minu-Plus**

  This can be used for encryption and it is slower in decryption due to the search.

2.) Parallel generalization – HFE.

- The only difference from MI is that F is replaced by a new map given by:

$$F(X) = \sum_{i,j=0}^{D} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{D} b_i X^{q^i} + c.$$

- To invert this map, one needs to use the Berlakemp algorithm to solve the polynomial equation:

$$F(X) = Y'.$$

- Due to the work of Kipnis, Shamir, Courtois, Faugere, Joux, etc, D cannot be too small. Therefore, the system is much slower.
- Work by Stern, Jous, Granboulan at Crypto 2006.

3.) LE generalization – XL, which is closed related to the new Gröbner basis methods F_4 and F_5 by Faugère.

The basic idea is very simple: to generate the ideal by multiplying monomial.

Given $f_1 = 0, .., f_n = 0$, we look for single variable polynomials in the span of $\{mf_i\}$, where m is a monomial of degree less or equal to a fix degree d.

d decides the efficiency of the algorithm.

4.) LE inspiration – Oil & Vinegar, which is for signatures.

Oil-Vinegar polynomials.

$x_1, .., x_0$ Oil-variables.

$x'_1, ..., x'_v$ Vinegar variables.

$$\sum a_{ij} x_i x'_j + \sum b_{ij} x'_i x'_j + \sum c_i x_i + \sum d_i x'_j + e$$

OV map is from k^{o+v} to k^o.

This map is easy to ”invert”.

1. Balanced case: $o = v$

It is broken by Kipnis – Shamir

The basic method is to search for a common invariant subspace of a set of matrices.

2. Unbalanced case: $v > o$.

5.) Combination of HFE and Oil & Vinegar – HFEv.

6.) HFE$^-$ – Quartz, a very short signature scheme.

Encryption scheme is harder to build than the signature schemes.

2.3 Internal Perturbation

2.3.1 General Idea

- (Internal) Perturbation was introduced at PKC 2004 as a general method to improve the security of multivariate public key cryptosystems.
- Construction – small-scale "noise" is added to the system in a controlled way so as to not fundamentally alter the main structure, but yet substantially increase the "entropy."
- $q = 2$.

2.4 Perturbation Agents

- Let r be a small integer and

$$z_1(x_1, \ldots, x_n) = \sum_{j=1}^{n} \alpha_{j1} x_j + \beta_1$$

$$\vdots$$

$$z_r(x_1, \ldots, x_n) = \sum_{j=1}^{n} \alpha_{jr} x_j + \beta_r$$

  be a set of randomly chosen affine linear functions in the x_i over k^n such that the $z_j - \beta_j$ are linearly independent.

- Let

$$Z(x_1, \ldots, x_n) = (z_1, \ldots, z_r) = (\sum_{j=1}^{n} \alpha_{j1} x_j + \beta_1, \ldots, \sum_{j=1}^{n} \alpha_{jr} x_j + \beta_r),$$

  a map from k^n to k^r.

2.5 Perturbation of MI

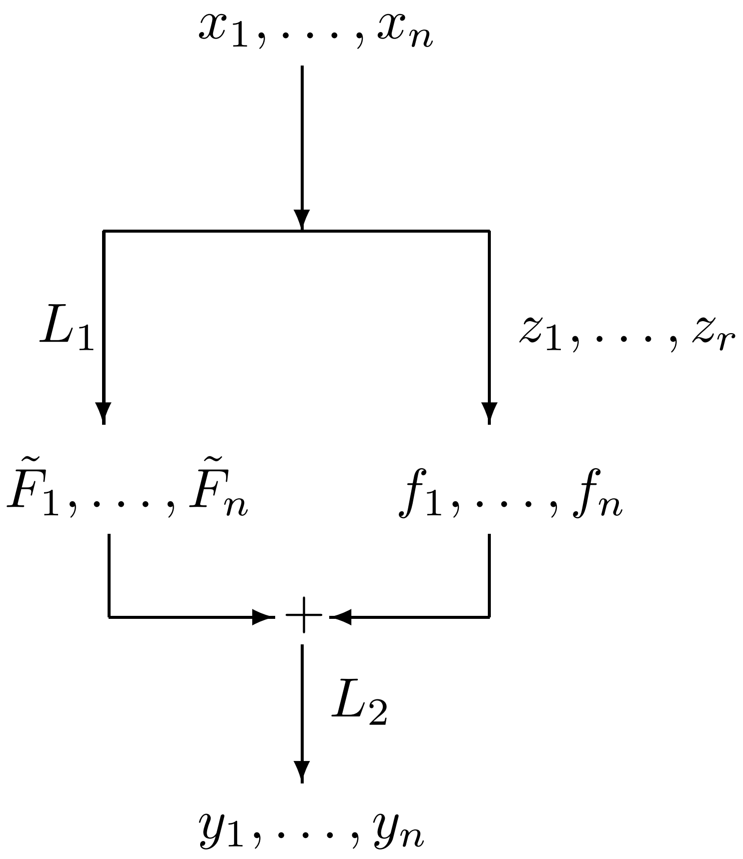

Figure 1: Structure of Perturbation of the Matsumoto-Imai System.

- The Construction:

$$\begin{aligned}
&\overset{=}{F}\ (x_1, \ldots, x_n) = (\overset{=}{F}_1\ (x_1, \ldots, x_n), \ldots, \overset{=}{F}_n\ (x_1, \ldots, x_n)) \\
&= (\tilde{F}_1(x_1, \ldots, x_n) + f_1(z_1, .., z_r), \ldots, \\
&\qquad \tilde{F}_n(x_1, \ldots, x_n) + f_n(z_1, \ldots, z_r)),
\end{aligned}$$

where the f_i are randomly chosen quadratic polynomials in r variables.

- $f(z_1, .., z_r) = (f_1(z_1, \ldots, z_r), \ldots, f_r(z_1, \ldots, z_r))$ can be viewed as a map from k^r to k^n – "the noise."
- Let P be the set consisting of the pairs (λ, μ), where λ is a point that belongs to the image of f, and μ is the pre-image of λ by f.
- We call P the perturbation set. P has q^r elements probabilistically, and it does not include any pair whose first component is the zero vector.

- $\bar{\bar{F}}$ is called the perturbation of $\tilde{F}$ by Z.
- r is the perturbation dimension.

2.5.1 The Public Key

The public key includes:

1.) The field k including its additive and multiplicative structure;

2.) The n quadratic polynomials:

$$y_1(x_1, \ldots, x_n), \ldots, y_n(x_1, \ldots, x_n).$$

2.5.2 Encryption

Given a plaintext message vector $M = (x'_1, \ldots, x'_n)$, the ciphertext is the vector

$$(y'_1, \ldots, y'_n) = (y_1(x'_1, \ldots, x'_n), \ldots, y_n(x'_1, \ldots, x'_n)).$$

2.5.3 The Private Key

The private key includes:

1.) The map F.

2.) The set of affine linear functions $z_1, \ldots, z_r$.

3.) The set of points in P (or equivalently, the set of the polynomials $f_i(z_1, .., z_r)$).

4.) The two affine linear maps L_1, L_2.

2.5.4 Decryption

For any ciphertext $(y'_1, \ldots, y'_n)$, the decryption includes the following steps:

I.) Compute $(\bar{y}_1, \ldots, \bar{y}_i) = L_1^{-1}(y'_1, \ldots, y'_n)$.

II.) One by one, take all the elements (λ, μ) in P, and compute $(y_{\lambda 1}, \ldots, y_{\lambda n}) = \phi^{-1} \circ F^{-1}((\bar{y}_1, \ldots, \bar{y}_i) + \lambda)$. Check if $Z(y_{\lambda 1}, \ldots, y_{\lambda n})$ is the same as the corresponding μ: if no, discard it; if yes, go to next step.

III.) Compute $(x_{\lambda 1}, \ldots, x_{\lambda n}) = L_2^{-1} \circ \phi(y_{\lambda 1}, \ldots, y_{\lambda n})$.

If there is only one solution, it is the plaintext. However, it is possible that there is more than one solution: we can use the same technique suggested for HFE, namely we can use hash functions to differentiate which is the correct one. This system is called the perturbed Matsumoto-Imai cryptosystem (PMI).

2.6 Previous attack

- Existing structural methods can not work effectively against PMI including the Gröbner bases-type attacks – F_4, F_5 and XL.

2.6.1 New Attack – Differential Attack

The new method that can effectively attack perturbation is the differential analysis method developed recently by Pierre-Alain Fouque, Jacques Stern and Louis Granboulan, which appeared in Eurocrypt 2005.

$$L_v(x) = \bar{F}(x+v) + \bar{F}(x) + \bar{F}(v) + \bar{F}(0),$$

For a given instance of PMI. It is straightforward to show that L_v is linear in x.

Let $\mathcal{K}$ be the "noise kernel," the kernel of the linear part of the affine transformation $Z \circ L_2$.

Then it can also be shown that

$$v \in \mathcal{K} \to \dim\left(\ker\left(L_v\right)\right) = \gcd\left(\theta, n\right).$$

If $v \notin \mathcal{K}$, then the dimension of the kernal of L_v has different statistical behavior.

- The differential attack amounts to finding a basis for $\mathcal{K}$ using this difference in statistical behavior, followed by q^r MI-type attacks, each attack being against PMI restricted to one of the q^r affine planes parallel to $\mathcal{K}$.
- The basic idea is actually to denoise ”the perturbation” , and then break the system

2.7 How to resist the differential attack

- Differential analysis uses the fact that the difference of MI is too “pure” and can be used to differentiate what is the “noise.”
- Add some different kind of ”noise” – randomly chosen quadratics to MI, then add internal perturbation.

  These two processes are commutative

$$\bar{F} = \bar{L}_1 \circ (\bar{\bar{F}}, P_1, (x_1, .., x_n) ... P_A(x_1, .., x_n)) \circ L_2,$$

where $\bar{L}_1$ is now a invertible affine map over k^{n+a}.

- The plus polynomials are "mixed" into the system.

- Adding random polynomial – the plus method — **external perturbation**
- If we add enough plus polynomials, then we can not see anymore the statistical difference of the behavior of the kernel.
- Adding too many makes the system susceptible to the Gröbner basis attack.

- For the practical example, we show that in general, the plus should be

$$A = g.c.d(n, \theta) + 10$$

  to ensure the security level at 2^{80}.

- The plus polynomials are also used to solve the problem of multiple candidates for the plaintext.
- The new system is called PMI+

- For practical use, we suggest that

  $n > 95$, $r = 6$.

- Implementation test shows that it in general 10 times faster than RSA (1024 bits) and in decryption process, it can be more than 10 times faster.

  Research group in Taiwan

2.8 Other related Work

- Internal Perturbation of HFE.

  (HFEv – External Perturbation.)

  PMI and IPHFE are very different in terms of the role of linear terms.

  IPHFE is much faster than HFE.

  Good resistance to differential attack.

- This IP method is recently used by CHABANNE, DOTTAX , BRINGER to improve a multivariate traitor tracing schemes by Gilbert.

2.9 TTM

1) Tame transformation Method by T.T. Moh.

The basic idea is to use tame transformation or triangular map:

$$G(x_1, ..., x_n) = (x_1, x_2 + g_1(x_1), x_3 + g_2(x_1, x_2),$$

$$..., x_n + g_{n-1}(x_1, ..., x_{n-1}).$$

Jacobian conjecture, Nagata problem.

The main ides:

$$G(x_1, ..., x_n) = L_1 \circ T_1 \circ T_2 \circ L_2,$$

where one of the T_1, T_2 is upper-triangular and the other lower triangular.

The subtlety is the degree 2 requirement, which is a subtle combinatorical problem.

TTMs are all broken by now.

2.10 Rainbow-TTS-STS

Multi-layer Oil-Vinger – TTM^-.

Rainbow, TTS, TRMC

TTS uses sparse Oil-viegar polynomials, and signing can be 100 times faster than RSA.

2.11 MFE

Middle field equation (MFE)- Wang, Yang, Hu etc – RSA 2006.

It is broken. Ding, Hu, etc.

One big field — Several field of middle size.

2.12 Zhuang-zi algorithm

The idea is to lift a set of multivariate equations into a single variable equation, and try to solve it.

3 Challenges

- New Structures

  MI – Big Field

  Middle Field Equation – MFE – Middle Field

  TTM –Triangular Maps. (Jacobian Conjecture)

  Can we make TTM work?

  New algebraic structures we could explore?

- Geneneral attack

  Groebner basis

  F_4, F_5

  XL

  Zhuang-zi

  Complexity?

  Why can HFE be defeated by F_4?

- Applications

  Small devices – passive RFID.

  Short-coming: large public key

  How to overcome this problem?

- Provable security

  Different attack methods.

  1) Polynomial equation solving.

  2) Rank.

  Minrank problem.

My Commercial:

A book:

Multivariate public key cryptosystems.

was just published in Springer's **Information Security** series.

Authors:

Jintai Ding, Dieter Schmidt, Jason Gower

Thanks and Questions?