MQ Challenge: Hardness Evaluation of Solving MQ Problems

Takanori Yasuda (ISIT), Xavier Dahan (ISIT),
Yun-Ju Huang (Kyushu Univ.), Tsuyoshi Takagi (Kyushu Univ.),
Kouichi Sakurai (Kyushu Univ., ISIT)

This work was supported by "Strategic Information and Communications R&D Promotion Programme (SCOPE), no. 0159-0091", Ministry of Internal Affairs and Communications, Japan. The first author is supported by Grant-in-Aid for Young Scientists (B), Grant number 24740078.

Fukuoka MQ challenge

MQ challenge started on April 1st.

https://www.mqchallenge.org/

Why we need MQ challenge?

- Several public key cryptosystems held contests which solve the associated basic mathematical problems.
  - RSA challenge(RSA Laboratories), ECC challenge(Certicom), Lattice challenge(TU Darmstadt)
- Lattice challenge (http://www.latticechallenge.org/)
  - Target: Short vector problem
  - 2008 – now continued
- Multivariate public-key cryptsystem (MPKC) also need to evaluate the current state-of-the-art in practical MQ problem solvers.

We planed to hold MQ challenge.

Multivariate Public Key Cryptosystem (MPKC)

- **Advantage**
  - Candidate for post-quantum cryptography
  - Used for both encryption and signature schemes
    - Encryption: Simple Matrix scheme (ABC scheme), ZHFE scheme
    - Signature: UOV, Rainbow
  - Efficient encryption and decryption and signature generation and verification.
- **Problems**
  - <u>Exact estimate of security of MPKC schemes</u>
  - Huge length of secret and public keys in comparison with RSA
  - New application and function

MQ problem

MPKC are public key cryptosystems whose security depends on the difficulty in solving a system of multivariate quadratic polynomials with coefficients in a finite field K.

MQ problem: find a solution of the system of multivariate equations:

$$
\begin{cases}
f_1(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d_1 \\
f_2(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d_2 \\
\vdots \\
f_m(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d_m
\end{cases}
$$

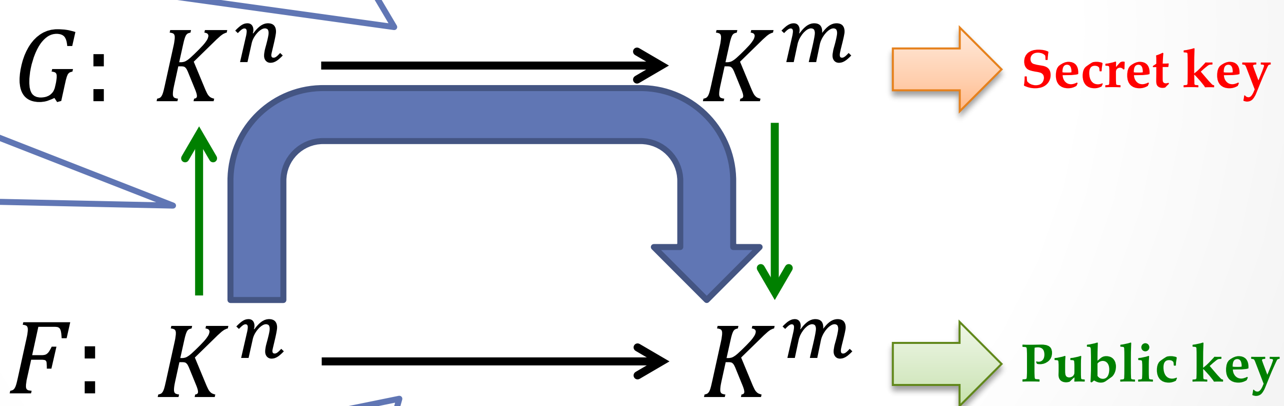
It is believed that it is difficult to solve (general) MQ problem.

MPKC Structure

Trapdoor one-way function

1. Choose a multivariate quadratic polynomial map whose inverse can be computed easily.

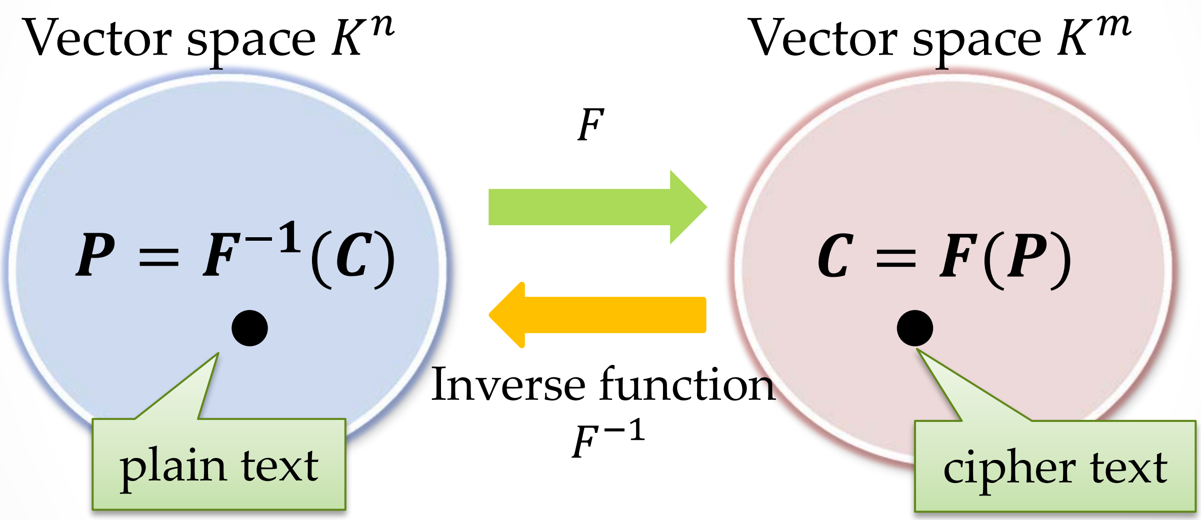
2. Choose two affine transformations.



3. Define a multivariate polynomial map by the composition of F and two affine transformations.

MPKC Encryption

$F: K^n \to K^m$: multivariate polynomial map



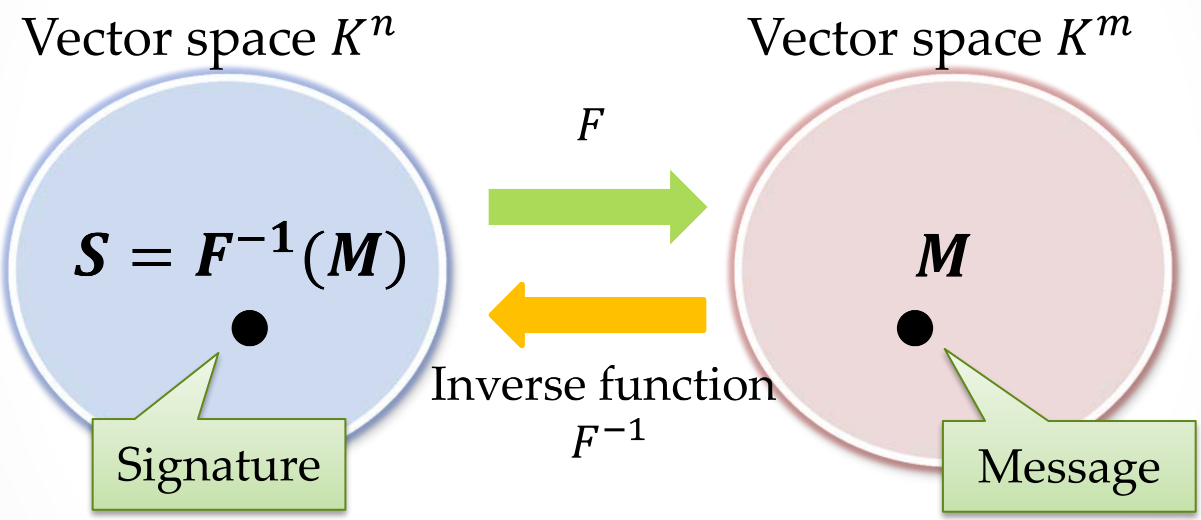
For any cipher text *C*, there must exist the corresponding plain text uniquely.

⇒ F is injective. ⇒ $n \leq m$.

Ex. Simple Matrix scheme, ZHFE

MPKC Signature

$F: K^n \to K^m$: multivariate polynomial map



For any message $\boldsymbol{M}$, there must exist the corresponding signature.

⇒ F is surjective. ⇒ $n \geq m$. Ex. UOV, Rainbow

Encryption and Signature

- Encryption
  - Simple matrix scheme(ABC scheme), ZHFE, ...
  - These encryption schemes use systems of $m = 2n$.
  - QUAD stream cipher also uses systems of $m = 2n$.
- Signature
  - UOV, Rainbow,…
  - Rainbow is the multilayered UOV.
  - In Rainbow, parameters $n \fallingdotseq 1.5m$ are often used.

- In MPKC schemes, finite fields with small size are used.
  - Finite field with small size has an efficient arithmetic.
  - Binary field $GF(2)$, binary extension field $GF(2^8)$, prime field $GF(31)$.

Systems of 6 types

- We create sequences of MQ problems of 6 types.

Type	Relation of m and n	Base field	Target
I	$m = 2n$	$GF(2)$	Encryption
II	$m = 2n$	$GF(2^8)$	Encryption
III	$m = 2n$	$GF(31)$	Encryption
IV	$n \approx 1{,}5m$	$GF(2)$	Signature
V	$n \approx 1{,}5m$	$GF(2^8)$	Signature
VI	$n \approx 1{,}5m$	$GF(31)$	Signature

How to construct MQ problem (Type IV,V,VI)

Signature Case ($n \approx 1.5m$)

Expected number of solutions of random system : $q^{1.5m-m} = q^{0.5m}$

$$\begin{cases} f_1(x_1,\dots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_{ij}^{(1)} x_i + c^{(1)} = d^{(1)}, \\ f_2(x_1,\dots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_{ij}^{(2)} x_i + c^{(2)} = d^{(2)}, \\ \vdots \\ \vdots \\ f_m(x_1,\dots,x_n) = \sum_{1\le i\le j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_{ij}^{(m)} x_i + c^{(m)} = d^{(m)}. \end{cases}$$

Step 1: choose randomly all coefficients .

How to construct MQ problem (Type I,II,III)

Encryption Case ($m = 2n$)

Existence probability of solution of random system : $1/q^n$

$$\begin{cases} f_1(x_1, \dots, x_n) = \sum_{1 \le i \le j \le n} a_{ij}^{(1)} x_i x_j + \sum_{1 \le i \le n} b_{ij}^{(1)} x_i + c^{(1)} = d^{(1)}, \\ f_2(x_1, \dots, x_n) = \sum_{1 \le i \le j \le n} a_{ij}^{(2)} x_i x_j + \sum_{1 \le i \le n} b_{ij}^{(2)} x_i + c^{(2)} = d^{(2)}, \\ \vdots \\ \vdots \\ f_m(x_1, \dots, x_n) = \sum_{1 \le i \le j \le n} a_{ij}^{(m)} x_i x_j + \sum_{1 \le i \le n} b_{ij}^{(m)} x_i + c^{(m)} = d^{(m)}. \end{cases}$$

Step 1: choose randomly blue coefficients .

Step 2: choose randomly a solution $v = (v_1, \dots, v_n)$.

Step 3: compute the red vector by evaluating polynomials at v.

This system has at least one solution v.

Gröbner basis attack

A fundamental tool for solving MQ problem is Gröbner basis. Faugère proposed efficient algorithms as F_4 and F_5 to improve original algorithm[1][2].

Complexity for solving MQ problem [3]

$$\mathcal{O}\left(\left(m \cdot \binom{n + d_{reg}}{d_{reg}}\right)^{\omega}\right)$$

where $2 < \omega < 3$, and d_{reg} is an invariant determined by the multivariate polynomial system.

Reference:

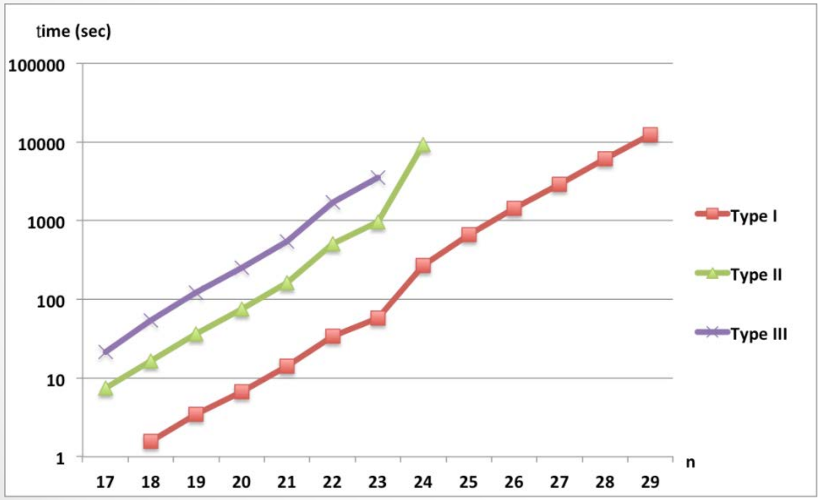
[1] Faugère, J.C., A New Efficient Algorithm for Computing Gröbner Bases (F4)", Journal of Pure and Applied Algebra, vol. 139, 1999.

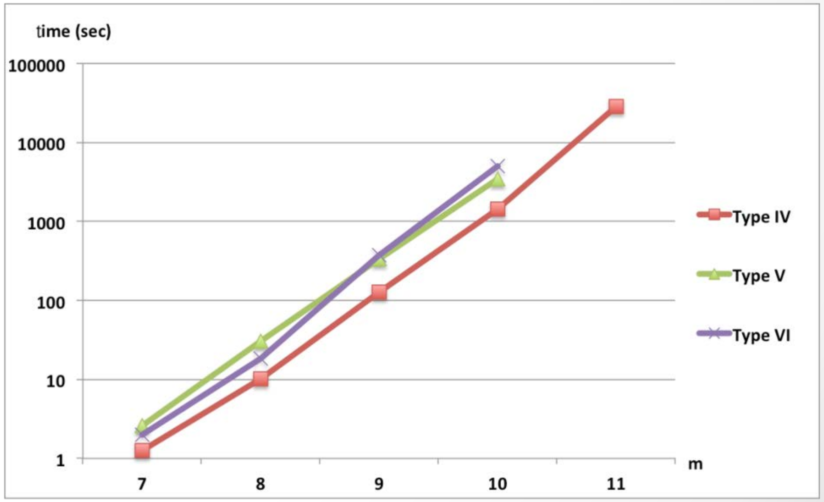
[2] Faugère, J.C., A New Efficient Algorithm for Computing Gröbner Bases (F5)", ISSAC, ACM press, 2002.

[3] Bettale, L., Faugère, J.C. and Perret L., Hybrid approach for solving multivariate systems over finite fields", J. Math. Crypt. vol. 2, 2008.

Experiments

- CPU: Intel(R) Xeon(R) CPU E5-4617, 2.90GHz, 6 cores
- OS: Linux Mint 15 Olivia
- RAM: 1TB
- Platform: Magma V2.19-9





Fukuoka MQ challenge

MQ challenge started on April 1st.

https://www.mqchallenge.org/

First Answerer

Participants Info

Name	JC Faugere
Institute	INRIA

Submission Details

Date	2015/4/1
Type	VI
Number of variables (n)	24
Number of equationes (m)	16
Seed (0,1,2,3,4)	0
Algorithm	F5 - FGb
Hardware	Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz
Running Time	5280 seconds
Answer $v=[v_1,\ldots,v_n]$ in F^n	[3,4,16,4,1,0,11,2,6,23,16,26,6,23,2,1,17,30,21,5,17,0,24,9]

Conclusion

- We started MQ challenge which is a contest for solving MQ problem.
    - MQ Challenge Homepage.

      https://www.mqchallenge.org/

PQCrypto 2016

- 2006 Leuven, 2008 Cincinnati, 2010 Darmstadt, 2011 Taipei, 2013 Limoges, 2014 Waterloo
- Seventh International Conference on Post-Quantum Cryptography
  February 24-26, 2016, Fukuoka, Japan
  https://pqcrypto2016.jp/
- Winter School
  February 22-23, 2016, Fukuoka, Japan

Fukuoka, Japan

Venue: Kyushu University
Nishijin Plaza

Thank you for your attention.