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.
  o RSA challenge (RSA Laboratories), ECC challenge (Certicom), Lattice challenge (TU Darmstadt)

• Lattice challenge (http://www.latticechallenge.org/)
  o Target: Short vector problem
  o 2008 – now continued

• Multivariate public-key cryptosystem (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**
  - Exact estimate of security of MPKC schemes
  - 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:

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

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

Trapdoor one-way function

$G : K^n \rightarrow K^m$

Secret key

$F : K^n \rightarrow K^m$

Public key
MPKC Encryption

\[ F : K^n \rightarrow K^m : \text{multivariate polynomial map} \]

Vector space \( K^n \)

\[ P = F^{-1}(C) \]

Plain text

Vector space \( K^m \)

\[ C = F(P) \]

Cipher text

For any cipher text \( C \), there must exist the corresponding plain text uniquely.

\[ F \text{ is injective.} \quad n \leq m. \quad \text{Ex. Simple Matrix scheme, ZHFE} \]
MPKC Signature

\[ F: K^n \rightarrow K^m : \text{multivariate polynomial map} \]

For any message \( M \), there must exist the corresponding signature.

\[ S = F^{-1}(M) \]

\( F \) is surjective. \( n \geq m \).

Ex. UOV, Rainbow
Encryption and Signature

• Encryption
  o Simple matrix scheme (ABC scheme), ZHFE, ....
  o These encryption schemes use systems of $m = 2n$.
  o QUAD stream cipher also uses systems of $m = 2n$.

• Signature
  o UOV, Rainbow,…
  o Rainbow is the multilayered UOV.
  o In Rainbow, parameters $n \approx 1.5m$ are often used.

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

2015/4/3 ETSI Quantum Safe Workshop
Systems of 6 types

- We create sequences of MQ problems of 6 types.

<table>
<thead>
<tr>
<th>Type</th>
<th>Relation of $m$ and $n$</th>
<th>Base field</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>$m = 2n$</td>
<td>$GF(2)$</td>
<td>Encryption</td>
</tr>
<tr>
<td>II</td>
<td>$m = 2n$</td>
<td>$GF(2^8)$</td>
<td>Encryption</td>
</tr>
<tr>
<td>III</td>
<td>$m = 2n$</td>
<td>$GF(31)$</td>
<td>Encryption</td>
</tr>
<tr>
<td>IV</td>
<td>$n \approx 1.5m$</td>
<td>$GF(2)$</td>
<td>Signature</td>
</tr>
<tr>
<td>V</td>
<td>$n \approx 1.5m$</td>
<td>$GF(2^8)$</td>
<td>Signature</td>
</tr>
<tr>
<td>VI</td>
<td>$n \approx 1.5m$</td>
<td>$GF(31)$</td>
<td>Signature</td>
</tr>
</tbody>
</table>
How to construct MQ problem (Type IV, V, VI)

Signature Case \( (n \approx 1.5m) \)

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

\[
\begin{align*}
    f_1(x_1, \ldots, x_n) &= \sum_{1 \leq i \leq j \leq n} a_{ij}^{(1)} x_i x_j + \sum_{1 \leq i \leq n} b_{ij}^{(1)} x_i + c^{(1)} = d^{(1)}, \\
    f_2(x_1, \ldots, x_n) &= \sum_{1 \leq i \leq j \leq n} a_{ij}^{(2)} x_i x_j + \sum_{1 \leq i \leq n} b_{ij}^{(2)} x_i + c^{(2)} = d^{(2)}, \\
    &\vdots \\
    f_m(x_1, \ldots, x_n) &= \sum_{1 \leq i \leq j \leq n} a_{ij}^{(m)} x_i x_j + \sum_{1 \leq i \leq n} b_{ij}^{(m)} x_i + c^{(m)} = d^{(m)}. 
\end{align*}
\]

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: \( 1/q^n \)

\[
\begin{align*}
    f_1(x_1, \ldots, x_n) &= \sum_{1 \leq i \leq j \leq n} a^{(1)}_{ij} x_i x_j + \sum_{1 \leq i \leq n} b^{(1)}_{ij} x_i + c^{(1)} = d^{(1)}, \\
    f_2(x_1, \ldots, x_n) &= \sum_{1 \leq i \leq j \leq n} a^{(2)}_{ij} x_i x_j + \sum_{1 \leq i \leq n} b^{(2)}_{ij} x_i + c^{(2)} = d^{(2)}, \\
    &\vdots \\
    f_m(x_1, \ldots, x_n) &= \sum_{1 \leq i \leq j \leq n} a^{(m)}_{ij} x_i x_j + \sum_{1 \leq i \leq n} b^{(m)}_{ij} x_i + c^{(m)} = d^{(m)}. \\
\end{align*}
\]

Step 1: choose randomly blue coefficients.
Step 2: choose randomly a solution \( v = (v_1, \ldots, v_n) \).
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]**

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

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

Reference:

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

<table>
<thead>
<tr>
<th>Name</th>
<th>JC Faugere</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institute</td>
<td>INRIA</td>
</tr>
</tbody>
</table>

## Submission Details

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

• We started MQ challenge which is a contest for solving MQ problem.
  o MQ Challenge Homepage.
    https://www.mqchallenge.org/
PQCrypto 2016


- 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.