Overview of Quantum-Safe Cryptography

Ludovic Perret  J.-C. Faugère  Thomas Prest (TCS)
ludovic.perret@lip6.fr  jean-charles.faugere@inria.fr  thomas.prest@ens.fr

Quantum-Safe Cryptography for Industry (QsCI)

UPMC Sorbonne Universités  INRIA Paris  CNRS
Roadmap

1. What is Quantum-Safe (a.k.a Post-Quantum) Cryptography
2. Quantum-Safe Algorithmic Hard Problems (with Thomas Prest)
Quantum-Safe Cryptography

- Public-key cryptography = hard mathematical problems
- Dlog, Factorisation

Shor's Algorithm

Solves factoring and breaks RSA
Quantum-Safe Cryptography
Established Academic Topic

Goal. Design cryptographic primitives secure against classical and quantum computers.
Quantum-Safe Shift

global effort in quantum-safe

Mathematical Modelling for Next-Generation Cryptography

RISQ

we are here

2014

NSA/NIST announcements
Quantum-Safe Landscape

Quantum-Safe Landscape


- Lattice-based
- Isogeny-based
- Code-based
- Hash-based
- Quantum-key distribution
- Multivariate-based
Quantum-Safe Landscape

NIST anticipates that the evaluation process for these post-quantum cryptosystems may be significantly more complex than the evaluation of the SHA-3 and AES candidates. Finally, some of the candidate quantum-resistant cryptosystems may have completely different design attributes and mathematical foundations, so that a direct comparison of candidates would be difficult or impossible.

Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process (Draft)

www.nist.gov/pqcrypto
Posso Problem

Input. Non linear polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$

Question. Find – if any – $(z_1, \ldots, z_n) \in \mathbb{F}_q^n$

\[
\begin{aligned}
    p_1(z_1, \ldots, z_n) &= 0 \\
    \vdots \\
    p_m(z_1, \ldots, z_n) &= 0
\end{aligned}
\]

mostat is NP-Hard [Garey-Johnson]

« Random instances » of Posso
are hard to solve in practice

No (known) exponential quantum speedup
Multivariate Public-Cryptography

Family of schemes whose security is directly related to the difficulty of Posso

Many schemes proposed: HFE, QUARTZ (HFEv-), UOV, Rainbow, ....

T. Matsumoto, H. Imai.
« Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption ». EUROCRYPT '88.

J. Patarin.
« Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms ». EUROCRYPT '96.
Multivariate Public-Key Cryptography

[Matsumoto-Imai'88]

Secret-Key.

Easy to invert set of polynomials

\[
\begin{align*}
&f_1(x_1, \ldots, x_n) \\
&\vdots \\
&f_m(x_1, \ldots, x_n)
\end{align*}
\]

\[(S, T) \in \text{GL}_n(\mathbb{F}_q) \times \text{GL}_m(\mathbb{F}_q)\]

Public-Key.

\[
\begin{align*}
&p_1(x_1, \ldots, x_n) \\
&\vdots \\
&p_m(x_1, \ldots, x_n)
\end{align*}
\]

\[p = T \circ f \circ S\]
Multivariate Public-Key Cryptography

Secret-Key.

\[
\begin{align*}
  f_1(x_1, \ldots, x_n) \\
  \vdots \\
  f_m(x_1, \ldots, x_n)
\end{align*}
\]

\((S, T) \in \text{GL}_n(F_q) \times \text{GL}_m(F_q)\)

Decrypt

\[
m = S^{-1} \circ f^{-1} \circ T^{-1}(c).
\]

Public-Key.

\[
\begin{align*}
  p_1(x_1, \ldots, x_n) \\
  \vdots \\
  p_m(x_1, \ldots, x_n)
\end{align*}
\]

\[p = T \circ f \circ S\]

Encrypt

\[
c = p(m)
\]

we evaluate the message on the polynomials

\(m \approx n\)
Multivariate Public-Key Cryptography

Secret-Key.
\[
\begin{align*}
    f_1(x_1, \ldots, x_n) \\
                     \vdots \\
    f_m(x_1, \ldots, x_n)
\end{align*}
\]
\((S, T) \in \text{GL}_n(\mathbb{F}_q) \times \text{GL}_m(\mathbb{F}_q)\)

Generation
\[
s = S^{-1} \circ f^{-1} \circ T^{-1}(H).
\]

Public-Key.
\[
\begin{align*}
    p_1(x_1, \ldots, x_n) \\
                     \vdots \\
    p_m(x_1, \ldots, x_n)
\end{align*}
\]
\[p = T \circ f \circ S\]

 Verification
\[
H = p(s)
\]

We evaluate the signature

\(m < n\)
Hidden Field Equations


HFE Secret Polynomial

$D \in \mathbb{N}$ and $q$ prime.

$$F(X) = \sum_{0 \leq i \leq j < n} A_{i,j} X^{q^i + q^j} + \sum_{0 \leq i < n, q^i \leq D} B_i X^{q^i} + C \in \mathbb{F}_q[X].$$

$X = \sum_{i=1}^{n} x_i \theta_i$

Finding the zeroes of $f_1, \ldots, f_n \iff$ solve $F(X) = 0$
**Hidden Field Equations**


**HFE Secret Polynomial**

\( D \in \mathbb{N} \) and \( q \) prime.

\[
F(X) = \sum_{0 \leq i \leq j < n, \ q^i + q^j \leq D} A_{i,j} X^{q^i + q^j} + \sum_{0 \leq i < n, \ q^i \leq D} B_i X^{q^i} + C \in \mathbb{F}_{q^n}[X].
\]

**Decryption Timings [MacBook Pro, 2016]**

<table>
<thead>
<tr>
<th>(n,D)</th>
<th>Magma 2.19</th>
<th>(80,129)</th>
<th>(80,257)</th>
<th>(80,513)</th>
<th>(128,129)</th>
<th>(128,257)</th>
<th>(128,513)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.04 s.</td>
<td>0.09 s.</td>
<td>0.2 s.</td>
<td>0.05 s.</td>
<td>0.12 s.</td>
<td>0.32 s.</td>
<td></td>
</tr>
</tbody>
</table>
Known Attacks

- Message recovery attack [J.-C Faugère, A. Joux, 2003]
  - First HFE challenge broken (n = 80, q = 2, D = 96, 80 bits security)
  - Theoretical upper bound ([L. Granboulan, A. Joux, J. Stern, 2006], [V. Dubois, N. Gamma, 2011], [J. Ding, T. Hodges, 2012], . . . )
- Differential properties [T. Daniels, D. Smith-Tone]
- . . . . .

All known attack are exponential in log(D)
Selecting Parameters

Direct Attack

The complexity of a message-recovery attack against a HFE with secret polynomial of degree D with Gröbner bases is bounded by:

\[ O(n^{\log_q(D) \omega}) \]

with \(2 \leq \omega \leq 3\) the linear algebra constant.


Structural Attack

Under a genericity assumption, the complexity of a key-recovery attack against a HFE with secret polynomial of degree D with Gröbner bases is:

\[ O\left(n^{(\log_q(D)+1) \omega}\right) \]

HFEBoost Project

- PoC android application tested by French army
- Key Transport with a variant of HFE (HFEBoost)
Real-Life Deployment

- Basic file encryption app. (Key-transport+AES)
- Deployed in Samsung devices
- Dedicated 4G networks
**HFEBest in Practice**

- **HFE-**, \( n=127 \) variables, 125 equations, secret Boost polynomial of degree \( D=3072 \)
- Sparte polynomial
- **HFE-** public-key size: 130 KB for 80 bits of security
- Dedicated ARM implementation of RootsFinding (J.-C. Faugère)

<table>
<thead>
<tr>
<th>Device</th>
<th>KEX (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung Galaxy S5</td>
<td>0.72</td>
</tr>
<tr>
<td>Samsung Galaxy S6 (32 bits)</td>
<td>0.49</td>
</tr>
<tr>
<td>MacBook Pro</td>
<td>0.18</td>
</tr>
</tbody>
</table>
# Multivariate-based Cryptography

Design principle. Security based on the hardness of solving a system of non-linear equations

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
<th>PK Size</th>
<th>Signature Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption/Key-transport</td>
<td>Versatile design</td>
<td>Bad reputation, many schemes broken</td>
<td>60 – 400 Kbytes</td>
</tr>
<tr>
<td>Signature MI</td>
<td>Signature verification (fast), small signature size</td>
<td>Medium size of the pk</td>
<td></td>
</tr>
<tr>
<td>Signature ZK</td>
<td>Based on random PoSSO</td>
<td>Large signature</td>
<td></td>
</tr>
</tbody>
</table>

M.-S Chen and A. Hülsing, J. Rijneveld, S. Samardjiska, P. Schwabe. From 5-pass MQ-based identification to MQ-based signatures. Asiacrypt'16.

No attack on these schemes.
## Code-based Cryptography

**Design principle.** Security based on the hardness of decoding a linear code

<table>
<thead>
<tr>
<th>Pro</th>
<th>Co</th>
<th>PK size</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>McEliece — Binary goppa Codes</strong></td>
<td>key-transport (fast), signature, encryption (fast)+oldest quantum-safe cryptosystem (1976)</td>
<td>signature process is slow, size of the public-key</td>
</tr>
<tr>
<td><strong>McEliece — Quasi-cyclic MDPC codes</strong></td>
<td>key-transport (fast), signature (slow), encryption (fast), size of the pk</td>
<td>New hardness assumption (2013)</td>
</tr>
</tbody>
</table>

---


