Gröbner Bases Techniques in Post-Quantum Cryptography

Ludovic Perret

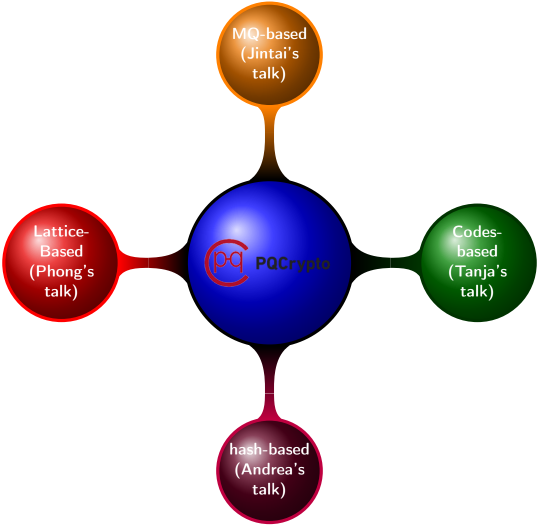
Sorbonne Universités, UPMC Univ Paris 06, INRIA Paris
LIP6, PolSyS Project, Paris, France

Post-Quantum Cryptography Winter School, Fukuoka, Japan

PQCrypto 2016

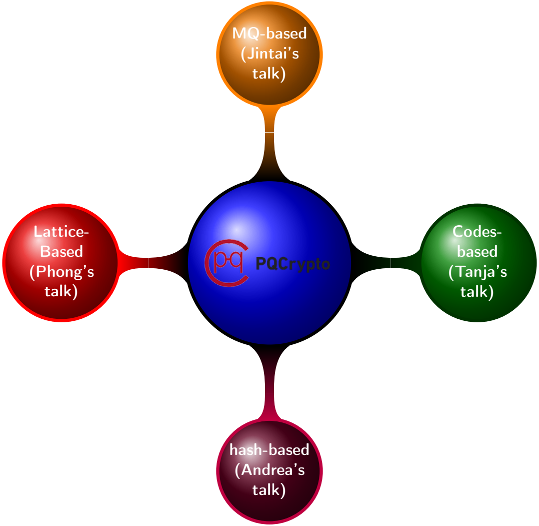
Post-Quantum Revolution

- NIST aims to standardize quantum-resistant algorithms within 2020
    - Main challenge is to understand precisely the hardness.

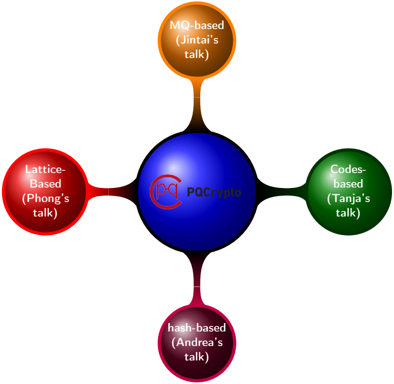


Post-Quantum Revolution

Gröbner bases is a major tool for quantum resistant schemes



Post-Quantum Revolution

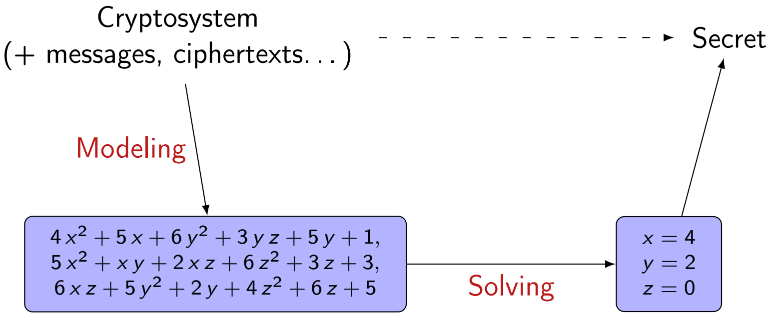


- Multivariate : intrinsic tool
- Code-based : emerging tool
  - J.-C. Faugère, V. Gauthier-Umana, A. Otmani, L. P., J.-P. Tillich.
    A Distinguisher for High Rate McEliece Cryptosystems.
    IEEE-IT 13.
  - A. Couvreur, A. Otmani, J.-P. Tillich.
    Polynomial Time Attack on Wild McEliece over Quadratic Extensions.
    EUROCRYPT 2014.
  - J.-C. Faugère, A. Otmani, L. P., F. De Portzamparc, J.-P. Tillich.
    Structural Cryptanalysis of McEliece Schemes with Compact Keys.
    DCC'2015.
  - PQC'16 program (Rank codes, Polar Codes)
- `LWE`-based : new tool for asympt. hardness
- Hash-based : minor impact

Algebraic Cryptanalysis

Idea

- **Model** a cryptosystem as a set of algebraic equations
- Try to **solve** this system (code-based, multivariate based), or **estimate** the difficulty of solving (`LWE`)
  - $\Rightarrow$ Gaussian Elimination, Gröbner basis, SAT-solver...
  - N. Courtois, J. Ding, J.-C. Faugère, W. Meier, J. Patarin, A. Shamir, B.-Y. Yang ...



Polynomial System Solving (PoSSo)

q, size of field $\quad$ n, nb. of variables $\quad$ m, nb. of equations

PoSSo

Input. non-linear polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$
Question. Find – if any – $(z_1, \ldots, z_n) \in \mathbb{F}_q^n$ such that:

$$\begin{cases} p_1(z_1, \ldots, z_n) = 0, \\ \vdots \\ p_m(z_1, \ldots, z_n) = 0\,. \end{cases}$$

Remark

- PoSSo is NP-hard
- Random instances of PoSSo are hard to solve in practice.

PoSSo Fukuoka Challenges

- https://www.mqchallenge.org

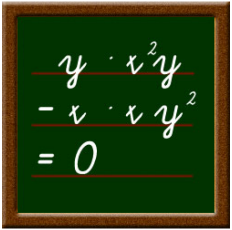
Methodology

Difficulties

- Modeling : describe a cryptosystem as a set of algebraic of equations
  - "universal" approach (PoSSo is NP-Hard)
    - ⇒ several models are possible !!!
- Solving
  - ⇒ Minimize the number of variables/degree
  - ⇒ Maximize the number of equations

Specificity

- cryptographic context
- Gröbner bases



Gröbner Basis

Linear system	Non linear system
$\begin{cases} \ell_1(x_1,\ldots,x_n)=0 \\ \ldots \\ \ell_m(x_1,\ldots,x_n)=0 \end{cases}$	$\begin{cases} p_1(x_1,\ldots,x_n)=0 \\ \ldots \\ p_m(x_1,\ldots,x_n)=0 \end{cases}$
$V = \mathrm{Vec}_{\mathbb{F}_q}(\ell_1,\ldots,\ell_m)$	$\mathcal{I} = \langle f_1,\ldots,f_m\rangle$
Gauss reduction of V	Gröbner basis $\mathcal{I}$

Definition [B. Buchberger'1965]

Let $\prec$ be a mon. ordering (LEX or DRL), and $\mathcal{I} \subset \mathbb{F}_q[x_1,\ldots,x_n]$.
$G \subset \mathcal{I}$ is a Gröbner basis iff:

$$\forall f \in \mathcal{I} \quad \exists g \in G \text{ such that } \mathrm{LeadingTerm}_{\prec}(g) \,|\, \mathrm{LeadingTerm}_{\prec}(f).$$

Zero-Dimensional Strategy

$$\begin{array}{ccc} p_1(x_1,\dots,x_n) & & g_1(x_1,\dots,x_n) \\ \vdots & \underset{\text{compute GB}}{\Longrightarrow} & \vdots \\ p_m(x_1,\dots,x_n) & & g_s(x_n) \end{array}$$

Initial syst. LEX-GB

Zero-Dimensional Strategy

$$
\begin{array}{ccccc}
p_1(x_1,\ldots,x_n) & & g'_1(x_1,\ldots,x_n) & & g_1(x_1,\ldots,x_n) \\
\vdots & \underset{\text{compute GB}}{\Longrightarrow} & \vdots & \underset{\text{change order}}{\Longrightarrow} & \vdots \\
p_m(x_1,\ldots,x_n) & & g'_r(x_1,\ldots,x_n) & & g_s(x_n) \\
\text{Initial syst.} & & \text{DRL-GB} & & \text{LEX-GB}
\end{array}
$$

Computing a Gröbner Basis

B. Buchberger
"An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal", PhD thesis, 1965.

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

J.-C. Faugère.
"A New Efficient Algorithm for Computing Gröbner bases Without Reduction to Zero (F5)."
ISSAC, 2002.

... ⋮

C. Eder and J.-C. Faugère.
"A Survey on Signature-Based Gröbner Basis Computations".
ArXiv, April 2014.

B. Buchberger.

Computing a Gröbner Basis

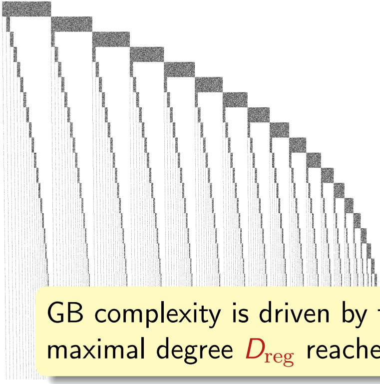
Macaulay Matrix $\mathcal{M}^{\text{acaulay}}_{d,m}$ of degree d

- $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$
- $\prec$ monomial ordering (LEX, or DRL)
- $t_{i,j}$ monomials of degree $d - \deg(f_i)$

$$
\begin{array}{c}
\\
t_{1,1}\,p_1 \\
t_{1,2}\,p_1 \\
\vdots \\
t_{m,1}\,p_m \\
t_{m,2}\,p_m \\
\vdots
\end{array}
\quad
\begin{array}{c}
\text{mono. of deg.} \leqslant D \text{ sorted for } \prec \\
\left(
\begin{array}{c}
\\
\\
\ldots\ldots\ldots \\
\ldots\ \mathrm{Coeff}(t\,p_i, \prec)\ \ldots \\
\vdots \\
\ldots\ldots\ldots \\
\ldots\ldots\ldots
\end{array}
\right)
\end{array}
$$

Polynomial System Solving

Macaulay matrix $\mathcal{M}^{\mathrm{acaulay}}_{d,m}$ in degree d



GB complexity is driven by the maximal degree D_{reg} reached

$p_1 = \cdots = p_m = 0$

Gaussian Elimination of matrices up to degree D_{reg}

- Buchberger (1965
- F_4 (1999)
- F_5 (2002)
- . . .

$O(\binom{n+D_{\mathrm{reg}}}{n}^{\omega})$

Gröbner: total degree

- FGLM (1993)

$\tilde{O}(\#Sols^3)$

Gröbner: lexicographical

GBLA

- GBLA team: B. Boyer, C. Eder, J.-C Faugère, F. Martani
- `http://www-polsys.lip6.fr/~jcf/GBLA/index.html`

GBLA

Presentation

GBLA is an open source (GPLv2) C library for linear algebra specialized for eliminating matrices generated during Gröbner basis computations in algorithms like F4 or F5.

Download source

Current stable source (version 0.0.3).

In order to use it, you can proceed as follows :

```
tar xf gbla-x.y.z.tar.gz
cd gbla-x.y.z
./autogen.sh
./configure
make
```

The `configure` step can be customised. Help is provided with `configure --help` and can be used like `configure CFLAGS="-march=native -O3"` to replace default `"-g -O2"`.

If you need the tools :

```
cd tools ; make ;
```

Usage

- **Programme `gbla`**

  See usage for detailed help, and the following for a few examples.

  Example:

  ```
  zcat mat1.gz | ./gbla -
  ```

  Computes the eliminations, uses 1 thread, outputs nothing, uses the old format, reads from the gunzipped stream `mat1.gz`.

  ```
  zcat matrices/mat1.gbm.gz | ./gbla -v 1 -t 4 -
  ```

  Computes the eliminations, uses 4 threads, outputs minimal information, uses the new format, reads from the gunzipped stream `matrices/mat1.gbm.gz`.

  ```
  ./gbla -v 2 -t 32 -n matrices/mat1.gbm
  ```

  Computes the eliminations, uses 32 threads, outputs timings and information, uses the new format, reads from a matrix `mat1` on disk.

  Binaries

  Compiled binaries can be found there:
  - linux (Intel static)
  - linux (Intel AVX static)

Complexity

Degree of Regularity

Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be homogeneous polynomials.

$$D_{\mathrm{reg}} = \min_d \left\{ \dim_{\mathbb{K}}(\{p \in \langle p_1, \ldots, p_m \rangle \mid \deg(p) = d\}) = \binom{n+d-1}{d} \right\}.$$

Complexity

Semi-Regular Sequence [Bardet, Faugère, Salvy, Yang, MEGA'2003]

$p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ $(m > n)$ be hom. polynomials of degree d. If the system is *semi-regular*, then D_{reg} is the index of the first non-positive coeff. $\leqslant 0$

$$\sum_{d \geqslant 0} h_d \, z^d = \frac{(1 - z^d)^m}{(1 - z)^n}$$

- h_d rank defects of $\mathcal{M}^{\mathrm{acaulay}}_{d,m}$
- Only trivial relations $p_i p_j = p_j p_i$
- For non-homogenous polynomials, homogeneous part of highest degree
- *Fröberg's conjecture* : semi-regular sequences exist !

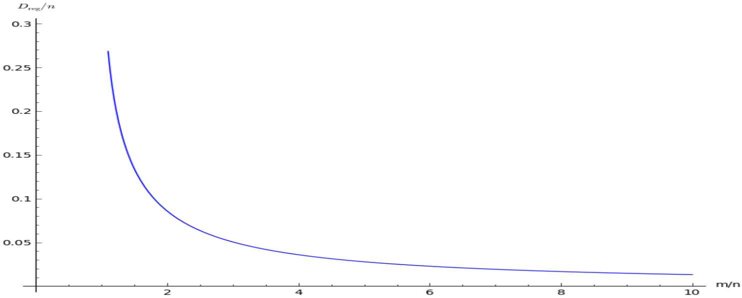
Example $(n = 5, m = 6, d = 2)$

$$1 + 5\,x + 9\,x^2 + 5\,x^3 - 4\,x^4 + \ldots$$

Asymptotic Expansion [Bardet, Faugère, Salvy, Yang, MEGA'2003]

Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a semi-regular system of $m = C \cdot n$ quadratic equations with $C > 1$ a constant :

$$D_{\text{reg}} \approx \left(C - \frac{1}{2} - \sqrt{C(C-1)} \right) n.$$

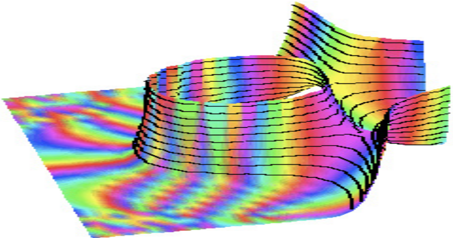


Complexity

Global Picture [Bardet, Faugère, Salvy, Research Report, 2003]

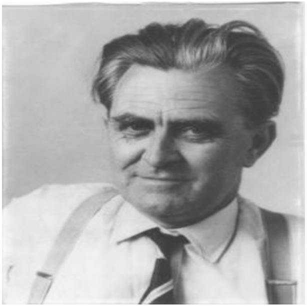
Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a semi-regular system of m quadratic equations:

- poly-time complexity if $m = \binom{n+2}{2}$ (Linearization bound)
- poly-time complexity for GB if $m = \binom{n+1}{2}$
- sub-exponential complexity if $m = \tilde{O}(n)$
- exponential complexity if $m = O(n)$ or $m = n + \mathrm{Cst}$



Plan

1. **Algebraic Algorithms for LWE Problems (joint work with M. Albrecht, C. Cid, J.-C Faugère)**
   - Linear Equations with Noise $\mapsto$ Noise-Free Algebraic Equations
   - A Gröbner Basis Algorithm for BinaryErrorLWE
2. **Gröbner Bases Techniques in MPQC (joint work with L. Bettale, and J.-C Faugère)**
   - MinRank Attack on HFE
   - Solving MinRank
3. **Real-Life Deployment of Multivariate Cryptography (joint work with J.-C Faugère)**



W. Gröbner.

Learning With Errors (LWE)

$\texttt{LWE}(\alpha)$

Input. a random matrix $G \in \mathbb{F}_q^{n\times m}$ and $\mathbf{c} \in \mathbb{F}_q^m$.
Question. Find – if any – a secret $(s_1, \ldots, s_n) \in \mathbb{F}_q^n$ such that:

$$\textbf{error} = \mathbf{c} - (s_1, \ldots, s_n) \times G \in \mathbb{F}_q^m \text{ is ``}\textit{small}\text{''}.$$

- ☞ $q \in \mathrm{poly}(n)$, prime
- ☞ **special error distribution** s.t. $|\,\textbf{error}_i\,| \leqslant \alpha q \ll q$
- ☞ Many cryptosystems based on LWE
- ☞ Connection to **worst-case** GAPSVP $\alpha \cdot q \geqslant \sqrt{n}$

O. Regev.
"On Lattices, Learning with Errors, Random Linear Codes, and Cryptography".
Journal of the ACM, 2009.

Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé.
"Classical Hardness of Learning with Error".
STOC 2013.

LWE with Binary Errors

BinaryErrorLWE

Input. a random matrix $G \in \mathbb{F}_q^{n \times m}$ and $\mathbf{c} \in \mathbb{F}_q^m$.
Question. Find – if any – a secret $(s_1, \ldots, s_n) \in \mathbb{F}_q^n$ such that:

$$\textbf{error} = \mathbf{c} - (s_1, \ldots, s_n) \times G \in \{0, 1\}^m.$$

N. Döttling, J. Müller-Quade.
"Lossy Codes and a New Variant of the Learning with Errors Problem".
Eurocrypt'13.

D. Micciancio, C. Peikert.
"Hardness of SIS and LWE with Small Parameters".
CRYPTO'13.

LWE with Binary Errors

D. Micciancio, C. Peikert.
"Hardness of SIS and LWE with Small Parameters".
CRYPTO'13.

BinaryErrorLWE

Input. a random matrix $G \in \mathbb{F}_q^{n\times m}$ and $\mathbf{c} \in \mathbb{F}_q^m$.
Question. Find – if any – a secret $(s_1, \ldots, s_n) \in \mathbb{F}_q^n$ such that:

$$\mathbf{error} = \mathbf{c} - (s_1, \ldots, s_n) \times G \in \{0, 1\}^m.$$

Hardness Results

- ✔ Reduction from BinaryErrorLWE with $m = n\left(1 + \Omega(1/\log(n))\right)$ to the worst-case Gap-SVP
- ☞ [Arora-Ge'10] Proven polynomial-time algorithm by linearization if $m \in O(n^2)$

Algebraic Cryptanalysis

- **Model** BinaryErrorLWE as a set of non-linear equations
  - ⇒ [Arora-Ge'10,] Linear Equations **with noise** to **noise-free** algebraic equations
- **Solve** this system and estimate the difficulty of solving
  - ⇒ [Arora-Ge'10, Ding'10] Linearization
  - ⇒ Complexity analysis with Gröbner bases under a genericity assumption
  - ⇒ Hardness of BinaryErrorLWE for $n\left(1+\Omega(1/\log(n))\right) < m < O(n^2)$.
  - ⇒ Exp. speed up w.r.t. to Arora-Ge for $\texttt{LWE}(\alpha)$

S. Arora, and R. Ge.
"New Algorithms for Learning in Presence of Error".
ICALP'11 & Electronic Colloquium on Computational Complexity, April 2010.

J. Ding.
"Solving LWE Problem with Bounded Errors in Polynomial Time".
IACR Cryptology ePrint Archive, November 2010.

Plan

1. **Algebraic Algorithms for LWE Problems (joint work with M. Albrecht, C. Cid, J.-C Faugère)**
   - Linear Equations with Noise $\mapsto$ Noise-Free Algebraic Equations
   - A Gröbner Basis Algorithm for BinaryErrorLWE
2. **Gröbner Bases Techniques in MPQC (joint work with L. Bettale, and J.-C Faugère)**
   - MinRank Attack on HFE
   - Solving MinRank
3. **Real-Life Deployment of Multivariate Cryptography (joint work with J.-C Faugère)**

Algebraic Modelling

BinaryErrorLWE

Input. a random matrix $G \in \mathbb{F}_q^{n \times m}$, and $\mathbf{c} \in \mathbb{F}_q^m$.
Question. Find – if any – $(s_1, \ldots, s_n) \in \mathbb{F}_q^n$ such that:

$$\mathbf{c} - (s_1, \ldots, s_n) \times G = \mathbf{error} \in \{0, 1\}^m.$$

☞ m **linear equations** in n variables over $\mathbb{F}_q$ **with binary noise**.

Algebraic Modelling

BinaryErrorLWE

Input. a random matrix $G \in \mathbb{F}_q^{n \times m}$, and $\mathbf{c} \in \mathbb{F}_q^m$.
Question. Find – if any – $(s_1, \ldots, s_n) \in \mathbb{F}_q^n$ such that:

$$\mathbf{c} - (s_1, \ldots, s_n) \times G = \textbf{error} \in \{0,1\}^m.$$

☞ m **linear equations** in n variables over $\mathbb{F}_q$ **with binary noise**.

Arora-Ge (AG) Modelling

Let $P(X) = X(X-1)$:

$$p_1 = P\Big(c_1 - \sum_{j=1}^{n} s_j G_{j,1}\Big) = 0, \ldots, p_m = P\Big(c_m - \sum_{j=1}^{n} s_j G_{j,m}\Big) = 0.$$

☞ m **quadratic equations** in n variables over $\mathbb{F}_q$.

Until Now

- $P(X) = X(X-1) \in \mathbb{F}_q[X]$ be vanishing on the errors.

AG Modelling

Solving BinaryErrorLWE $\equiv$

$$p_1 = P\left(c_1 - \sum_{j=1}^{n} x_j G_{j,1}\right) = 0, \ldots, p_m = P\left(c_m - \sum_{j=1}^{n} x_j G_{j,m}\right) = 0.$$

AG algorithm

- BinaryErrorLWE: m quadratic equations in n variables over $\mathbb{F}_q$.
  - ✔ **Linearisation** $\mapsto$ polynomial-time algo. when $m = O(n^2)$.

Linear Independence

Theorem

Let $P(x) = X(X-1)$. If $q > 2m$, then for all $m, 1 \leqslant m \leqslant \binom{n+1}{2}$:

$$p_1 = P\Big(c_1 - \sum_{j=1}^{n} x_j G_{j,1}\Big), \ \ldots \ , p_m = P\Big(c_m - \sum_{j=1}^{n} x_j G_{j,m}\Big),$$

are linearly independent with probability $\geqslant 1 - \frac{2m}{q}$.

Linear Independence

Proof.

- Mat: a sub-matrix of size $m \times m$ of the Macaulay matrix at degree 2
- $p(G) = \mathrm{Det}(\mathrm{Mat})$.
- if $p(G)$ is non-zero, then by Schwartz-Zippel-DeMillo-Lipton:

$$\Pr_G(p(G) \neq 0) \geqslant 1 - \frac{2m}{q}.$$

- Find G^* such that $p(G^*) \neq 0$:

$$\begin{bmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$\square$

Plan

1. **Algebraic Algorithms for LWE Problems (joint work with M. Albrecht, C. Cid, J.-C Faugère)**
    - Linear Equations with Noise $\mapsto$ Noise-Free Algebraic Equations
    - A Gröbner Basis Algorithm for BinaryErrorLWE
2. **Gröbner Bases Techniques in MPQC (joint work with L. Bettale, and J.-C Faugère)**
    - MinRank Attack on HFE
    - Solving MinRank
3. **Real-Life Deployment of Multivariate Cryptography (joint work with J.-C Faugère)**

Solving BinaryErrorLWE with Gröbner Bases

Assumption

Systems occurring in the AGD modelling are semi-regular.

☞ Rank condition on the Macaulay matrices.

Solving BinaryErrorLWE with Gröbner Bases

Asymptotic Expansion

Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a semi-regular system of $m = C \cdot n$ quadratic equations with $C > 1$:

$$D_{\mathrm{reg}} \approx \left(C - \frac{1}{2} - \sqrt{C(C-1)} \right) n.$$

Theorem

Under the **semi-regularity assumption**:

- If $m = n\left(1 + \frac{1}{\log(n)}\right)$, one can solve BinaryErrorLWE in $\mathcal{O}\left(2^{3.25 \cdot n}\right)$.
- If $m = 2 \cdot n$, BinaryErrorLWE can be solved in $\mathcal{O}\left(2^{1.02 \cdot n}\right)$.
- If $m = \mathcal{O}\left(n \log \log n\right)$, one can solve BinaryErrorLWE in $\mathcal{O}\left(2^{\frac{3n \log\log\log n}{8 \log\log n}}\right)$.

About the Assumption

Assumption

Systems occurring in the Arora-Ge modelling are semi-regular.

☞ Rank condition on the Macaulay matrices.

Magma 2.19	D_{reg}	D_{real}	Time
$n \in \{5, \ldots, 25\}$ $\quad m = n \cdot \log_2(n)$	3	3	$\leqslant$ 24 sec.
$n \in \{26, \ldots, 53\}$ $\quad m = n \cdot \log_2(n)$	4	4	$\leqslant$ 6 days
$n = 60$ $\quad m = 709 \left(2\, n \log_2(n)\right)$	3	3	32 min.
$n = 100$ $\quad m = 1728 \left(2.6\, n \log_2(n)\right)$	3	3	40 h.

About the Assumption

Assumption

Systems occurring in the Arora-Ge modelling are semi-regular.

☞ Rank condition on the Macaulay matrices.

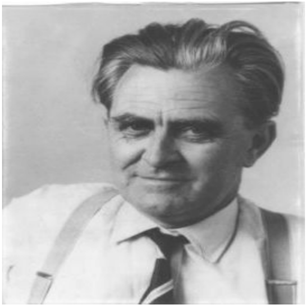
- Full proof of the assumption $\equiv$ proving the well known *Fröberg's conjecture*
- Semi-regularity of powers of generic linear forms [R. Fröberg, J. Hollman, JSC'94]
- Assumption proved in restricted cases

M. Albrecht, C. Cid, J.-C Faugère, L. Perret.
"Algebraic Algorithms for LWE".
IACR Eprint, 2014.

- Similar analysis for LWE(α)
  - $\Rightarrow$ Exp. speed up w.r.t. to Arora-Ge for LWE(α)

Plan

1. **Algebraic Algorithms for LWE Problems (joint work with M. Albrecht, C. Cid, J.-C Faugère)**
   - Linear Equations with Noise $\mapsto$ Noise-Free Algebraic Equations
   - A Gröbner Basis Algorithm for BinaryErrorLWE
2. **Gröbner Bases Techniques in MPQC (joint work with L. Bettale, and J.-C Faugère)**
   - MinRank Attack on HFE
   - Solving MinRank
3. **Real-Life Deployment of Multivariate Cryptography (joint work with J.-C Faugère)**



W. Gröbner.

Overview

- T. Matsumoto, H. Imai.
  "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption".
  EUROCRYPT '88.
- Jacques Patarin.
  Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms.
  EUROCRYPT '96.
- Prof. Takagi Group
  CryptoMathCREST project.
- Jintai's talk.

Multivariate Public-Key Cryptography

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

- Random instances of PoSSo are hard to solve in practice
- Many schemes proposed : HFE, UOV, Rainbow, ZHFE, Gui (HFEv-) ,. . .
  - MinRank attack on HFE

Overview

- T. Matsumoto, H. Imai. "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption". *EUROCRYPT '88.*
- Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. *EUROCRYPT '96.*
- Prof. Takagi Group CryptoMathCREST project.
- Jintai's talk.

Multivariate Public-Key Cryptography

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

- Random instances of PoSSo are hard to solve in practice
- Many schemes proposed : HFE, UOV, Rainbow, ZHFE, Gui (HFEv-) ,. . .
  - MinRank attack on HFE
- HFEBoost: Real-life deployment of multivariate cryptography

Private-Key

$\mathbf{f} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$ easy to invert.

$$f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$\vdots$$
$$f_n(x_1, \ldots, x_n).$$

$\mathbf{S}, \mathbf{T} \in \mathrm{GL_n}(\mathbb{F}_q)$.

Public-Key

$\mathbf{p} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$

$$p_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$\vdots$$
$$p_n(x_1, \ldots, x_n).$$

$\mathbf{p} = \mathbf{T} \circ \mathbf{f} \circ \mathbf{S}$.

Multivariate Public-Key Cryptography

Private-Key

$\mathbf{f} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$ easy to invert.

$$f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$\vdots$$
$$f_n(x_1, \ldots, x_n).$$

$\mathbf{S}, \mathbf{T} \in \mathrm{GL_n}(\mathbb{F}_q)$.

Public-Key

$\mathbf{p} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$

$$p_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$\vdots$$
$$p_n(x_1, \ldots, x_n).$$

$\mathbf{p} = \mathbf{T} \circ \mathbf{f} \circ \mathbf{S}$.

Encrypt:

$$\underline{c} = \mathbf{p}(\underline{m}).$$

Multivariate Public-Key Cryptography

Private-Key

$\mathbf{f} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$ easy to invert.

$$f_1(x_1, \dots, x_n),$$
$$\vdots$$
$$\vdots$$
$$f_n(x_1, \dots, x_n).$$

$\mathbf{S}, \mathbf{T} \in \mathrm{GL_n}(\mathbb{F}_q)$.

Decrypt:

$$\underline{m} = \mathbf{S}^{-1} \circ \mathbf{f}^{-1} \circ \mathbf{T}^{-1}(\underline{c}).$$

Public-Key

$\mathbf{p} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$

$$p_1(x_1, \dots, x_n),$$
$$\vdots$$
$$\vdots$$
$$p_n(x_1, \dots, x_n).$$

$\mathbf{p} = \mathbf{T} \circ \mathbf{f} \circ \mathbf{S}$.

Encrypt:

$$\underline{c} = \mathbf{p}(\underline{m}).$$

Jacques Patarin.
Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms.
EUROCRYPT '96.

HFE polynomial (q, prime)

Let $D \in \mathbb{N}$.

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

Decryption timings [J.-C. Faugère, Research Report, 2002]

- Roots

(n, D)	$(80, 129)$	$(80, 257)$	$(80, 513)$	$(128, 129)$	$(128, 257)$	$(128, 513)$
NTL	0.6 s.	2.5 s.	6.4 s.	1.25	3.1 s.	9.05 s.

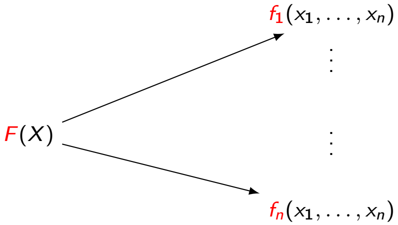
HFE Trapdoor

Jacques Patarin.
Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms.
EUROCRYPT '96.

HFE polynomial (q, prime)

Let $D \in \mathbb{N}$.

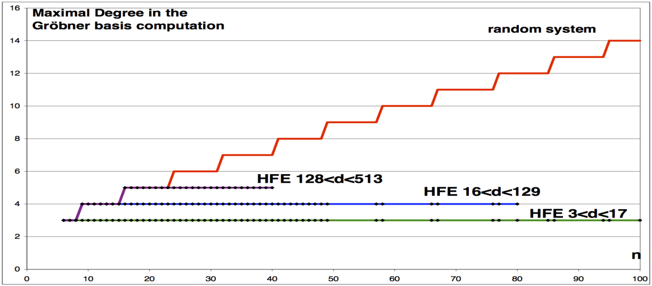
$$F(X) = \sum_{\substack{0 \leqslant i \leqslant j < n \\ q^i + q^j \leqslant D}} A_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leqslant i < n \\ q^i \leqslant D}} B_i X^{q^i} + C \in \mathbb{F}_{q^n}[X].$$



Some Known Attacks

- Message recovery attack [Faugère, Joux, 2003]
  - First HFE challenge broken in 2002 ($n = 80, q = 2, D = 96$, 80 bits security)
  - Theoretical degree of regularity ([L. Granboulan, A. Joux, J. Stern, 2006], [V. Dubois, N. Gamma, 2011], [J. Ding, T. Hodges, 2012], ...)
- Key recovery attack [A. Kipnis, A. Shamir, 1999, J. Ding, Schmidt, Werner, 2008]
- Weak keys [C. Bouillaguet, P.-A. Fouque, A. Joux, J. Treger, 2011]
- Differential properties [T. Daniels, D. Smith-Tone]
- ...

Message Recovery Attack



[Faugère, Joux; L. Granboulan, A. Joux, J. Stern; V. Dubois, N. Gamma; J. Ding, T. Hodges]

For any q:

$$D_{\text{reg}} = \mathcal{O}\big(\log_q(D)\big).$$

Outline

1. **Algebraic Algorithms for LWE Problems (joint work with M. Albrecht, C. Cid, J.-C Faugère)**
   - Linear Equations with Noise $\mapsto$ Noise-Free Algebraic Equations
   - A Gröbner Basis Algorithm for BinaryErrorLWE

2. **Gröbner Bases Techniques in MPQC (joint work with L. Bettale, and J.-C Faugère)**
   - MinRank Attack on HFE
   - Solving MinRank

3. **Real-Life Deployment of Multivariate Cryptography (joint work with J.-C Faugère)**

Rank Defect on F

Matrix Representation (non-standard quadratic form)

$$F(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{i,j} X^{q^i+q^j} = \underline{X}\mathbf{F}\underline{X}^t,$$

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

Rank Defect on F

Matrix Representation (non-standard quadratic form)

$$F(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{i,j} X^{q^i+q^j} = \underline{X}\mathbf{F}\underline{X}^t,$$

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

$$\begin{pmatrix} f_{1,1} & \ldots & f_{1,\ell} & 0 & \ldots & 0 \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ f_{\ell,1} & \ldots & f_{\ell,\ell} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

$q^i + q^j \leqslant D$

$\text{rank}(\mathbf{F}) = \log_q(\deg(F(X)))$.

A. Kipnis and A. Shamir.
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.
CRYPTO '99.

Rank Defects on the Public-key

Use directly the public quadratic forms $(p_1, \ldots, p_n)$.

Matrix Representation of Quadratic Form

$$p_1(x_1, \ldots, x_n) = \underline{x}\, \mathbf{G_1}\, \underline{x}^t$$

$$\vdots$$

$$p_n(x_1, \ldots, x_n) = \underline{x}\, \mathbf{G_n}\, \underline{x}^t,$$

with $\underline{x} = (x_1, \ldots, x_n)$.

L. Bettale, J.-C. Faugère, L. P.
Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants.
PKC 2011.

L. Bettale, J.-C. Faugère, L. P.
Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic.
DCC, 2012.

Linear change of basis between $(x_1, \ldots, x_n)$ and $(X^{q^0}, \ldots, X^{q^{n-1}})$

Proposition

Let $(\theta_1, \ldots, \theta_n) \in (\mathbb{F}_{q^n})^n$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

$$\mathbf{M}_n = \begin{pmatrix} \theta_1 & \theta_1^q & \ldots & \theta_1^{q^{n-1}} \\ \theta_2 & \theta_2^q & & \vdots \\ \vdots & & \ddots & \vdots \\ \theta_n & \theta_n^q & \ldots & \theta_n^{q^{n-1}} \end{pmatrix} \in \mathcal{M}_{n \times n}(\mathbb{F}_{q^n}).$$

- For $V = \sum_{i=1}^{n} v_i \theta_i \in \mathbb{F}_{q^n}$:

$$(v_1, \ldots, v_n)\, \mathbf{M}_n = (V, V^q, \ldots, V^{q^{n-1}}).$$

Improvement of Kipnis-Shamir's Attack

We write $\boxed{\mathbf{p} = \mathbf{T} \circ \mathbf{f} \circ \mathbf{S}}$ and $F(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{i,j} X^{q^i+q^j}$. Let $\mathbf{M}_n$

$$\begin{pmatrix} \theta_1 & \theta_1^q & \dots & \theta_1^{q^{n-1}} \\ \theta_2 & \theta_2^q & & \vdots \\ \vdots & & \ddots & \vdots \\ \theta_n & \theta_n^q & \dots & \theta_n^{q^{n-1}} \end{pmatrix} \in \mathcal{M}_{n \times n}\left(\mathbb{F}_{q^n}\right).$$

We have:

$$\underline{x}\mathbf{M}_n = (x_1, \dots, x_n)\mathbf{M}_n = (X, X^q, \dots, X^{q^{n-1}}), \text{with } X = \sum_{i=1}^n x_i \theta_i \in \mathbb{F}_{q^n}.$$

We define $p_k(\underline{x}) = \underline{x}\, \mathbf{G_k}\, \underline{x}^t$, $\mathbf{T}^{-1}\mathbf{M}_n = \mathbf{U} = [u_{i,j}]$, and $\mathbf{S}\,\mathbf{M}_n = \mathbf{W}$.

Fundamental Equation [L. Bettale, J.-C. Faugère, L. P., DCC'12]

$$\sum_{k=1}^{n} u_{k,0} \mathbf{G_{k+1}} = \mathbf{W}\mathbf{F}\mathbf{W}^t,$$

Improvement of Kipnis-Shamir's Attack

We write $\boxed{\mathbf{p} = \mathbf{T} \circ \mathbf{f} \circ \mathbf{S}}$ and $F(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{i,j} X^{q^i+q^j}$.

Fundamental Equation [L. Bettale, J.-C. Faugère, L. P., DCC'12]

$$\sum_{k=1}^{n} u_{k,0} \mathbf{G_{k+1}} = \mathbf{WFW}^t,$$

MinRank ([N. Courtois, 2001], [W. Buss, G. Frandsen, J. Shallit, 1999])

$\mathbf{G_0}, \ldots, \mathbf{G_{n-1}} \in \mathcal{M}_{n,n}(\mathbb{F}_q)$ and $r > 0$, find $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_q)^n$ s.t.

$$\operatorname{rank}\left(\sum_{k=1}^{n} \lambda_k \mathbf{G_k}\right) = r.$$

- MinRank in NP-hard

Outline

1. **Algebraic Algorithms for LWE Problems (joint work with M. Albrecht, C. Cid, J.-C Faugère)**
   - Linear Equations with Noise $\mapsto$ Noise-Free Algebraic Equations
   - A Gröbner Basis Algorithm for BinaryErrorLWE
2. **Gröbner Bases Techniques in MPQC (joint work with L. Bettale, and J.-C Faugère)**
   - MinRank Attack on HFE
   - Solving MinRank
3. **Real-Life Deployment of Multivariate Cryptography (joint work with J.-C Faugère)**

Solving MinRank – Kernel Approach

A. Kipnis, A. Shamir.
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.
CRYPTO 99.

The goal is to find $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_q^n$ s. t. :

$$\text{rank}\left(\sum_{j=1}^{n} \lambda_j M_j\right) = r.$$

- $E_\lambda = \sum_{j=1}^{n} \lambda_j M_j$:

$$\mathrm{Rk}(E_\lambda) = r \Leftrightarrow \exists (n-r) \text{ linearly indep. vectors } X^{(i)} \in \mathrm{Ker}(E_\lambda).$$

-

$$\left(\sum_{j=1}^{n} \lambda_j M_j\right) X^{(i)} = \mathbf{0}_n,\ \forall 1 \leqslant i \leqslant n-r.$$

Kernel Attack – (II)

- $E_\lambda = \sum_{j=1}^{n} \lambda_j M_j$.

$$\mathrm{Rk}(E_\lambda) = r \Leftrightarrow \exists (n-r) \text{ linearly indep. vectors } X^{(i)} \in \mathrm{Ker}(E_\lambda).$$

- Let $X^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)})$, where $x_j^{(i)}$s are variables. Then :

$$\left(\sum_{j=1}^{k} y_j M_j\right) \begin{pmatrix} x_1^{(1)} & \cdots & x_1^{(n-r)} \\ x_2^{(1)} & \cdots & x_2^{(n-r)} \\ \vdots & \vdots & \vdots \\ x_n^{(1)} & \cdots & x_n^{(n-r)} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

Kernel Attack – (III)

- Write $X^{(i)} = (e_i, x_1^{(i)}, \ldots, x_r^{(i)})$, where $e_i \in \mathbb{F}_q^{n-r}$ and $x_j^{(i)}$s are var.

$$\left(\sum_{j=1}^{k} y_j M_j\right) \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \\ x_1^{(1)} & \cdots & \cdots & x_1^{(n-r)} \\ \vdots & \vdots & \vdots & \vdots \\ x_r^{(1)} & \cdots & \cdots & x_r^{(n-r)} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

- Kernel attack [N. Courtois, L. Goubin, 2000], exhaustive search on the kernel, $O(q^{\frac{n\,r}{(n-r)}})$

Kernel Attack – (III)

- $\boxed{\text{Write } X^{(i)} = (e_i, x_1^{(i)}, \dots, x_r^{(i)})}$, where $e_i \in \mathbb{F}_q^{n-r}$ and $x_j^{(i)}$s are var.

$$\left(\sum_{j=1}^{k} y_j M_j\right) \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \\ x_1^{(1)} & \cdots & \cdots & x_1^{(n-r)} \\ \vdots & \vdots & \vdots & \vdots \\ x_r^{(1)} & \cdots & \cdots & x_r^{(n-r)} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

- Kernel attack [N. Courtois, L. Goubin, 2000], exhaustive search on the kernel, $O(q^{\frac{n\,r}{(n-r)}})$
- quadratic system of $(n-r)n$ equations in $r(n-r)+n$ unknowns.

J.-C. Faugère, F. Levy-dit-Vehel, L P.
Cryptanalysis of MinRank.
Crypto 2008.

Solving MinRank

$$\mathbf{G} = \sum_{i=1}^{n} \lambda_k \mathbf{G_i},$$

n: size of the matrices, **r**: target rank

Kipnis-Shamir modeling

$\textbf{Rank}(\mathbf{G}) = r \Leftrightarrow \exists x^{(1)}, \ldots, x^{(n-r)} \in \textbf{Ker}(\mathbf{G}).$

$$\mathbf{G} \cdot \begin{pmatrix} & I_{n-r} & \\ x_1^{(1)} & \ldots & x_1^{(n-r)} \\ \vdots & \vdots & \vdots \\ x_r^{(1)} & \ldots & x_r^{(n-r)} \end{pmatrix} = 0$$

- $n(n-r)$ multilinear equations.
- $r(n-r)+k$ variables.

Solving MinRank

$$\mathbf{G} = \sum_{i=1}^{n} \lambda_k \mathbf{G_i},$$

n: size of the matrices, **r**: target rank

Kipnis-Shamir modeling

$\mathbf{Rank}(\mathbf{G}) = r \Leftrightarrow \exists x^{(1)}, \ldots, x^{(n-r)} \in \mathbf{Ker}(\mathbf{G})$.

$$\mathbf{G} \cdot \begin{pmatrix} & I_{n-r} & \\ x_1^{(1)} & \ldots & x_1^{(n-r)} \\ \vdots & \vdots & \vdots \\ x_r^{(1)} & \ldots & x_r^{(n-r)} \end{pmatrix} = 0$$

- $n(n-r)$ multilinear equations.
- $r(n-r)+k$ variables.

Minors modeling

$$\mathbf{Rank}(\mathbf{G}) = r$$

$$\Updownarrow$$

all minors of size $(r+1)$ of $\mathbf{G}$ vanish.

- $\binom{n}{r+1}^2$ equations of degree $r+1$.
- k variables.

Few variables, lots of equations, high degree

Solving MinRank

$$\mathbf{G} = \sum_{i=1}^{n} \lambda_k \mathbf{G_i},$$

n: size of the matrices, **r**: target rank

Kipnis-Shamir modeling

$\mathbf{Rank}(\mathbf{G}) = r \Leftrightarrow \exists x^{(1)}, \ldots, x^{(n-r)} \in \mathbf{Ker}(\mathbf{G})$.

$$\mathbf{G} \cdot \begin{pmatrix} & I_{n-r} & \\ x_1^{(1)} & \ldots & x_1^{(n-r)} \\ \vdots & \vdots & \vdots \\ x_r^{(1)} & \ldots & x_r^{(n-r)} \end{pmatrix} = 0$$

- $n(n-r)$ multilinear equations.
- $r(n-r)+k$ variables.

Minors modeling

$$\mathbf{Rank}(\mathbf{G}) = r$$
$$\Updownarrow$$
all minors of size $(r+1)$ of $\mathbf{G}$ vanish.

- $\binom{n}{r+1}^2$ equations of degree $r+1$.
- k variables.

Few variables, lots of equations, high degree

J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer.
Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology.
ISSAC 2010.

Complexity Analysis – Minors

Proposition

- Let (n, k, r) be the parameters of MinRank and $\mathbf{A}(t) = [a_{i,j}(t)]$ be the $(r \times r)$-matrix defined by

$$a_{i,j}(t) = \sum_{\ell=0}^{n-\max(i,j)} \binom{n-i}{\ell}\binom{n-j}{\ell} t^{\ell}.$$

- The degree of regularity of MinRank polynomial systems is the index of the first $\leqslant 0$ coefficient in:

$$(1-t)^{(n-r)^2-k} \, \frac{\det \mathbf{A}(t)}{t^{\binom{r}{2}}}.$$

J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer.
Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology.
ISSAC 2010.

Solving HFE with MinRank

- $\log(\mathcal{C}_{\rm Gb}) = O(d_{\rm reg})$
- Explicit method to compute $d_{\rm reg}$ $\equiv$ Explicit method to bound the complexity of the Gröbner basis computation.

Theorem [L. Bettale, J.-C. Faugère, L. P., DCC'12]

Under a genericity assumption, the complexity of solving the `MinRank` on a `HFE` with secret polynomial of degree D with Gröbner bases:

$$\mathcal{O}\left(n^{(\log_q(D)+1)\,\omega}\right),$$

with $2 \leqslant \omega \leqslant 3$ the linear algebra constant.

Conclusion

- All known attacks against `HFE` are exponential in D.

Plan

1. Algebraic Algorithms for LWE Problems (joint work with M. Albrecht, C. Cid, J.-C Faugère)
   - Linear Equations with Noise $\mapsto$ Noise-Free Algebraic Equations
   - A Gröbner Basis Algorithm for BinaryErrorLWE
2. Gröbner Bases Techniques in MPQC (joint work with L. Bettale, and J.-C Faugère)
   - MinRank Attack on HFE
   - Solving MinRank
3. Real-Life Deployment of Multivariate Cryptography (joint work with J.-C Faugère)

Context

- PoC android application tested by French army
    - Key-Exchange with MPKC

Technology transfer

Mobile dev. compagny

Experiments on the battlefield

Is HFE Broken ?

Conclusion

- All known attacks against HFE are exponential in D.

Decryption timings [J.-C. Faugère, Research Report, 2002]

- Roots

(n, D)	$(80, 129)$	$(80, 257)$	$(80, 513)$	$(128, 129)$	$(128, 257)$	$(128, 513)$
NTL	0.6 s.	2.5 s.	6.4 s.	1.25	3.1 s.	9.05 s.

Conclusion

- All known attacks against HFE are exponential in D.

Decryption timings [J.-C. Faugère, Research Report, 2002]

- Roots

(n, D)	$(80, 129)$	$(80, 257)$	$(80, 513)$	$(128, 129)$	$(128, 257)$	$(128, 513)$
NTL	0.6 s.	2.5 s.	6.4 s.	1.25	3.1 s.	9.05 s.

Decryption timings [My laptop, 2016]

(n, D)	$(80, 129)$	$(80, 257)$	$(80, 513)$	$(128, 129)$	$(128, 257)$	$(128, 513)$
Magma 2.19	0.04 s.	0.09 s.	0.260 s.	0.05 s	0.12 s.	0.320 s.

Conclusion

- All known attacks against HFE are exponential in D.

Decryption timings [My laptop, 2016]

(n, D)	$(80, 129)$	$(80, 257)$	$(80, 513)$	$(128, 129)$	$(128, 257)$	$(128, 513)$
Magma 2.19	0.04 s.	0.09 s.	0.260 s.	0.05 s	0.12 s.	0.320 s.

[J.-C. Faugère, A. Joux, 2003]

The main result is that when the degree D of the secret polynomial is fixed, the cryptanalysis of an HFE system requires polynomial time in the number of variables. Of course, if D and n are large enough, **the cryptanalysis may still be out of practical reach**.

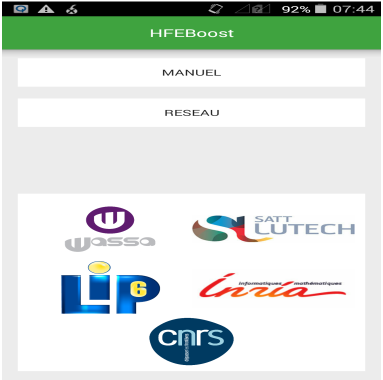
Characteristics

- HFE-, public-key size : 130 KB for 80 bits of security
- Dedicated ARM implementation of RootFinding (J.-C. Faugère)
- Patent in process

	Enc.	Dec.
Samsung Galaxy S5	mili s.	0.72 s.
Samsung Galaxy S6 (32 bits)	mili. s.	0.49 s.
Laptop (MAC)	milli. s.	0.18 s.

Conclusion

- MPKC is practical, good understanding of the security
- `HFEBoost`, early stage startup project
  - looking for more real-life experiments



jean-charles.faugere@inria.fr

ludovic.perret@lip6.fr