Gröbner Bases Techniques in Post-Quantum Cryptography

Ludovic Perret and many co-authors

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

NIST, Maryland

Gröbner Bases Techniques in Post-Quantum Cryptography

$\boxed{\text{A major tool to evaluate the security of post-quantum schemes}}$

- Multivariate cryptography: intrinsic tool (Jintai's talk)

Gröbner Bases Techniques in Post-Quantum Cryptography

A major tool to evaluate the security of post-quantum schemes

- Multivariate cryptography: intrinsic tool (Jintai's talk)
- Code-based cryptography: emerging tool for key-recovery

J.-C. Faugère, A. Otmani, L. P., J.-P. Tillich.
Algebraic Cryptanalysis of McEliece Variants with Compact Keys.
Eurocrypt 2010.

J.-C. Faugère, V. Gauthier-Umana, A. Otmani, L. P., J.-P. Tillich.
A Distinguisher for High Rate McEliece Cryptosystems.
IEEE-IT 13.

F. Urvoy.
Algebraic and Physical Cryptanalysis in Code-based Cryptography.
Paris VI.

Gröbner Bases Techniques in Post-Quantum Cryptography

$\boxed{\text{A major tool to evaluate the security of post-quantum schemes}}$

- Multivariate cryptography: intrinsic tool (Jintai's talk)
- Code-based cryptography: emerging tool for key-recovery

  J.-C. Faugère, A. Otmani, L. P., J.-P. Tillich.
  Algebraic Cryptanalysis of McEliece Variants with Compact Keys.
  Eurocrypt 2010.

  J.-C. Faugère, V. Gauthier-Umana, A. Otmani, L. P., J.-P. Tillich.
  A Distinguisher for High Rate McEliece Cryptosystems.
  IEEE-IT 13.

  F. Urvoy.
  Algebraic and Physical Cryptanalysis in Code-based Cryptography.
  Paris VI.
- LWE-based cryptography: new tool for asymptotical hardness

Algebraic Cryptanalysis

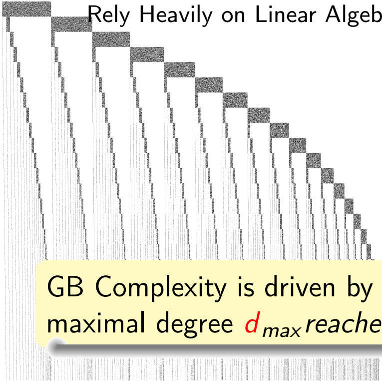
Idea

- Model a cryptosystem as a set of algebraic equations
- Try to solve this system, or estimate the difficulty of solving
  - $\Rightarrow$ Gaussian Elimination, Gröbner basis, ...

Polynomial System Solving

Matrix in degree d

Rely Heavily on Linear Algebra



GB Complexity is driven by the maximal degree d_{max} *reached*

$\boxed{f_1 = \cdots = f_m = 0}$

Gaussian Elimination of matrices up to degree d_{max}

$O(\binom{n+d_{max}}{n}^{\omega})$

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

$\boxed{\text{Gröbner: total degree}}$

Linear Algebra in $\mathbb{K}[\mathbf{x}]/I$ $\rightsquigarrow x_i = h_i(x_n)$

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

- FGLM (1993)

$\boxed{\text{Gröbner: lexicographical}}$

GBLA

- GBLA team: B. Boyer, **C. Eder**, J.-C Faugère, F. Martani.

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)

GBLA

- GBLA team: B. Boyer, **C. Eder**, J.-C Faugère, F. Martani.

GBLA

- GBLA team: B. Boyer, **C. Eder**, J.-C Faugère, F. Martani.

- Type VI, GF(31), $m = 16$, $n = 24$, GBLA: 2640 s. (FGB: 5280 s.)

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

Plan

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

Learning With Errors (LWE)

q : size of field	n : nb. of variables	m : nb. of samples

LWE

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:

$$\mathbf{error} = \mathbf{c} - (s_1, \ldots, s_n) \times G \text{ is "\textit{small}".}$$

☞ Decoding a random $[n, m]$ $\mathbb{F}_q$-linear code with a **special error distribution**.

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

LWE with Binary Errors

q : size of field	n : nb. of variables	m : nb. of samples

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:

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

- a prime $q \in \mathrm{poly}(n)$ $\big($for instance, $q = \mathrm{NextPrime}(n^2)\big)$,
- $m = n\big(1 + o(1)\big)$ is bounded

Hardness Results

- Gap-SVP is hard, even in the quantum setting.

BinaryErrorLWE [Micciancio-Peikert'13]

- ✔ Solving BinaryErrorLWE with $m = n \;\; 1 + o(1)$ allows to solve Gap-SVP in the worst-case
- ✔ Algos. for BinaryErrorLWE are exponential when $m = n \;\; 1 + o(1)$
  Polynomial-time algorithm if $m = O(n^2)$ (Arora-Ge'11)

Gröbner Bases Techniques

Arora-Ge'11

- ✔ Algebraic Modelling for `LWE`-problems
- ✔ Linearisation

Gröbner Bases Techniques

Arora-Ge'11

- ✔ Algebraic Modelling for `LWE`-problems
- ✔ Linearisation

Natural Idea

Complexity analysis of Arora-Ge equations with Gröbner bases.

Gröbner Bases Techniques

Arora-Ge'11

- ✔ Algebraic Modelling for `LWE`-problems
- ✔ Linearisation

Natural Idea

Complexity analysis of Arora-Ge equations with Gröbner bases.

Results [M. Albrecht, C. Cid, J.-C Faugère, L. P., "Algebraic Algorithms for `LWE`". IACR Eprint, 2014]

- `BinaryErrorLWE` is hard when $m = n \; 1 + o(1)$ ($\equiv$ `Gap-SVP`) and easy when $m = O(n^2)$.

A sub-exp. algorithm for `BinaryErrorLWE` when m is quasi-linear.

Plan

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

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:

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

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:

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

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

Arora-Ge Modelling

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

$$f_1 = P\left(c_1 - \sum_{j=1}^{n} s_j G_{j,1}\right) = 0, \ldots, f_m = P\left(c_m - \sum_{j=1}^{n} s_j G_{j,m}\right) = 0.$$

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

Until Now

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

Arora-Ge Modelling

Solving `BinaryErrorLWE` $\equiv$

$$f_1 = P\left(c_1 - \sum_{j=1}^{n} x_j G_{j,1}\right) = 0, \ldots, f_m = P\left(c_m - \sum_{j=1}^{n} x_j G_{j,m}\right) = 0.$$

Arora-Ge Algorithm

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

Plan

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

Solving `BinaryErrorLWE` with Gröbner Bases

Assumption

We assume that the systems occurring in the Arora-Ge modelling are semi-regular.

Rank condition on the Macaulay matrices.

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 $\mathcal{O}\left(2^{\frac{3n \log\log\log n}{8 \log\log n}}\right)$.

Solving `BinaryErrorLWE` with Gröbner Bases

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 $\mathcal{O}\left(2^{\frac{3n \log \log \log n}{8 \log \log n}}\right)$.

Remark

- Exact CVP/SVP solver: time $2^{0.377\, n}$ using memory $2^{0.029\, n}$.

A. Becker, N. Gama, A. Joux.
"Solving Shortest and Closest Vector Problems: the Decomposition Approach."
2013.

GB better when $m/n \geqslant 6.6$.

About the Assumption

Assumption

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

Rank condition on the Macaulay matrices.

Magma	D_{reg}	D_{real}
$m = n \cdot \log_2(n),\ n \in \{5, \ldots, 25\}$	3	3
$m = n \cdot \log_2(n),\ n \in \{26, \ldots, 53\}$	4	4
$m = 2 \cdot n \cdot \log_2(n),\ n = 60$	3	3
$m = 2 \cdot n \cdot \log_2(n),\ n = 100$	3	3

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

Conclusion

- Similar analysis for LWE
- New way to investigate the (asymptotical) hardness of lattice-based cryptography
- Main (challenging) open question is to prove the assumptions !

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