Impact of Quantum Computing to Cryptography
Part II

Ludovic Perret (`ludovic.perret@lip6.fr`)

Sorbonne University/CNRS
Co-founder of CryptoNext Security

Computability in Europe 2023, 24th-28th July 2023, Batumi, Georgia

Introduction & Organization of the Tutorial

Post-Quantum Cryptography

Cryptosystems secure both against classical and quantum adversaries

Part I. Cryptography in the era to quantum technologies

Part II. On the use of quantum algorithms in cryptanalysis

Polynomial System Solving over Finite Fields ($\texttt{PoSSo}_q$)

q, size of field	n, nb. of variables	m, nb. of equations

$\texttt{PoSSo}_q$

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:

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

Outline

1. Algebraic Cryptanalysis
2. $\texttt{PoSSo}_q$ and Gröbner bases
3. Algebraic cryptanalysis of $\texttt{LWE}$ with Binary Errors
4. Polynomial System Solving ($\texttt{PoSSo}_q$) in the Quantum Setting

Outline

1. Algebraic Cryptanalysis
2. $\texttt{PoSSo}_q$ and Gröbner bases
3. Algebraic cryptanalysis of $\texttt{LWE}$ with Binary Errors
4. Polynomial System Solving ($\texttt{PoSSo}_q$) in the Quantum Setting

Algebraic cryptanalysis

General approach to asses the security of post-quantum schemes

Idea

- **Model** a cryptosystem as a set of algebraic equations over a finite field ($\texttt{PoSSo}_q$ problem)
- Try to **solve** this system and/or **estimate** the difficulty of solving
  - ☞ N. Courtois, J. Ding, J.-C. Faugère, P.A. Fouque, H. Gilbert, L. Goubin, W. Meier, J. Patarin, I. Semaev, A. Shamir, B.-Y. Yang, . . .

Cryptosystem

(+ messages, ciphertexts, . . .) - - - - - - - → Secret

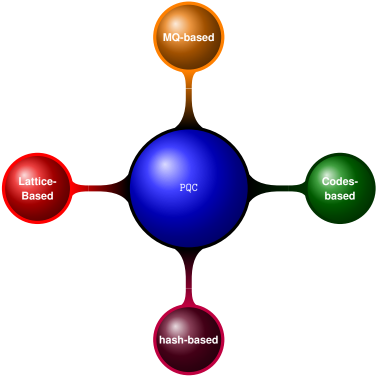
Modeling ↓

$$4x^2 + 5x + 6y^2 + 3yz + 5y + 1,$$
$$5x^2 + xy + 2xz + 6z^2 + 3z + 3,$$
$$6xz + 5y^2 + 2y + 4z^2 + 6z + 5$$

$\xrightarrow{\text{Solving } \texttt{PoSSo}_q}$

$$x = 4, \quad y = 2, \quad z = 0$$

Algebraic cryptanalysis



Multivariate : intrinsic tool

Code-based : important tool

Lattice-based : alternative tool for asympt. hardness

Hash-based : minor impact

Outline

1. Algebraic Cryptanalysis
2. $\texttt{PoSSo}_q$ and Gröbner bases
3. Algebraic cryptanalysis of $\texttt{LWE}$ with Binary Errors
4. Polynomial System Solving ($\texttt{PoSSo}_q$) in the Quantum Setting

Gröbner basis

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

- A monomial is a power product of the variables, i.e. an element of the form $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ ($x_1x_2x_3^{10}$ or $x_1x_2^2x_3$)

Definition [B. Buchberger'1965]

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

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

Gröbner basis

- A monomial is a power product of the variables, i.e. an element of the form $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ ($x_1x_2x_3^{10}$ or $x_1x_2^2x_3$)

Definition [B. Buchberger'1965]

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

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

- $x_1^{\alpha_1}\cdots x_n^{\alpha_n} \prec_{\mathrm{LEX}} x_1^{\beta_1}\cdots x_n^{\beta_n}$ if the first left-most nonzero entry of $\beta-\alpha$ is positive

$$x_1x_2x_3^{10} \prec_{\mathrm{LEX}} x_1x_2^2x_3$$

- $x_1^{\alpha_1}\cdots x_n^{\alpha_n} \prec_{\mathrm{DRL}} x_1^{\beta_1}\cdots x_n^{\beta_n}$ if $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, or $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ and the right-most nonzero entry of $\beta-\alpha$ is negative

$$x_1x_2x_3^{10} \succ_{\mathrm{DRL}} x_1x_2^2x_3$$

Gröbner basis

- A monomial is a power product of the variables, i.e. an element of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ ($x_1 x_2 x_3^{10}$ or $x_1 x_2^2 x_3$)

Definition [B. Buchberger'1965]

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

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

Definition

Let $\mathbb{F}_q \subseteq \mathbb{L}$ and $\mathcal{I} = \langle p_1, \ldots, p_m \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be an ideal.

$$V_{\mathbb{L}}(\mathcal{I}) = V_{\mathbb{L}}(p_1, \ldots, p_m) = \left\{ \mathbf{z} \in \mathbb{L}^n \mid p_i(\mathbf{z}) = 0, \forall i, 1 \leqslant i \leqslant m \right\},$$

is the $\mathbb{L}$-*variety* associated to $\mathcal{I}$.

☞ Usually, we want $\mathbb{L} = \mathbb{F}_q$, field equations $x_1^q - x_1, \ldots, x_n^q - x_n$ implicitly added

Gröbner basis

- A monomial is a power product of the variables, i.e. an element of the form $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ ($x_1x_2x_3^{10}$ or $x_1x_2^2x_3$)

Definition [B. Buchberger'1965]

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

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

Property

Let $\mathcal{I} = \langle p_1,\ldots,p_m\rangle \subset \mathbb{F}_q[x_1,\ldots,x_n]$ be a polynomial ideal. If $\#V(\mathcal{I}) = 1$, then – for any admissible monomial ordering – the (reduced) Gröbner basis G of $\mathcal{I}$ is as follows:

$$\{x_1 - a_1,\ldots,x_n - a_n\}, \text{ with } (a_1,\ldots,a_n) \in (\overline{\mathbb{F}_q})^n.$$

Zero-dimensional strategy

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

Initial syst. LEX-GB

Zero-dimensional strategy

$$\begin{matrix} p_1(x_1,\dots,x_n) \\ \vdots \\ p_m(x_1,\dots,x_n) \end{matrix} \quad \xRightarrow{\text{compute GB}} \quad \begin{matrix} g'_1(x_1,\dots,x_n) \\ \vdots \\ g'_r(x_1,\dots,x_n) \end{matrix} \quad \xRightarrow{\text{change order}} \quad \begin{matrix} g_1(x_1,\dots,x_n) \\ \vdots \\ g_s(x_n) \end{matrix}$$

Initial syst.

DRL-GB

LEX-GB

$\tilde{O}(\#\mathrm{Sols}^{\omega})$

FGLM [Faugère-Gianni-Lazard-Mora, 1993]

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

Figure: Bruno Buchberger

Gröbner basis & Linear algebra

Macaulay matrix $\mathcal{M}^{\mathrm{acaulay}}_{D,m}$ of degree D

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

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

Gröbner basis & Linear algebra

Lazard's theorem

Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a zero-dimensional (homogeneous) system. For D big enough, the row-echelon form of $\mathcal{M}^{\text{acaulay}}_{D,m}(p_1, \ldots, p_m)$ contains a Gröbner basis.

Complexity of computing a Gröbner basis – I

Complexity is driven by the maximal degree D_{reg} reached.

$$f_1 = \cdots = f_m = 0$$

- B. Buchberger (1965)
- D. Lazard (1983)
- F_4 (J.-C. Faugère, 1999)
- F_5 (J.-C. Faugère, 2002)
- FGLM (J-.C. Faugère, P. Gianni, D. Lazard, T. Mora, 1993)
- ...

$O\left(\binom{n+D_{\mathrm{reg}}}{D_{\mathrm{reg}}}^{\omega}\right)$, Row-echelon form on matrices up to degree D_{reg}

$$\downarrow$$

Variety

Complexity of computing a Gröbner basis – II

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

Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be quadratic homogeneous polynomials. The system is *regular* (resp. *semi-regular*) if $m \leqslant n$ (resp. $m > n$) and its Hilbert series is:

$$\frac{(1-z^2)^m}{(1-z)^n} = \sum_{i \geqslant 0} h_i \, z^i.$$

- ☞ h_i rank defects of $\mathcal{M}_{i,m}^{\mathrm{acaulay}}$
- ☞ D_{reg} is the index of the first coeff. $\leqslant 0$ of the Hilbert series.
- ☞ Extension to non-homogeneous polynomials $\rightarrow$ homogeneous components of highest degree

Complexity of computing a Gröbner basis – II

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

Let $p_1, \dots, p_m \in \mathbb{F}_q[x_1, \dots, x_n]$ be quadratic homogeneous polynomials. The system is *regular* (resp. *semi-regular*) if $m \leqslant n$ (resp. $m > n$) and its Hilbert series is:

$$\frac{(1-z^2)^m}{(1-z)^n} = \sum_{i \geqslant 0} h_i\, z^i.$$

- ☞ h_i rank defects of $\mathcal{M}_{i,m}^{\mathrm{acaulay}}$
- ☞ D_{reg} is the index of the first coeff. $\leqslant 0$ of the Hilbert series.
- ☞ Extension to non-homogeneous polynomials $\rightarrow$ homogeneous components of highest degree

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

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

Complexity of computing a Gröbner basis – II

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

Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be quadratic homogeneous polynomials. The system is *regular* (resp. *semi-regular*) if $m \leqslant n$ (resp. $m > n$) and its Hilbert series is:

$$\frac{(1-z^2)^m}{(1-z)^n} = \sum_{i \geqslant 0} h_i \, z^i.$$

- ☞ h_i rank defects of $\mathcal{M}^{\mathrm{acaulay}}_{i,m}$
- ☞ D_{reg} is the index of the first coeff. $\leqslant 0$ of the Hilbert series.
- ☞ Extension to non-homogeneous polynomials $\rightarrow$ homogeneous components of highest degree

- ❏ Regular sequence exists
- ❏ Randomly sampled instances of $\mathtt{PoSSo}_q$ behave as regular/semi-regular sequences
- ❏ Existence of semi-regular sequence is open (Fröberg's conjecture)

Complexity of computing a Gröbner basis – II

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

Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be quadratic homogeneous polynomials. The system is *regular* (resp. *semi-regular*) if $m \leqslant n$ (resp. $m > n$) and its Hilbert series is:

$$\frac{(1-z^2)^m}{(1-z)^n} = \sum_{i \geqslant 0} h_i \, z^i.$$

- ☞ h_i rank defects of $\mathcal{M}^{\mathrm{acaulay}}_{i,m}$
- ☞ D_{reg} is the index of the first coeff. $\leqslant 0$ of the Hilbert series.
- ☞ Extension to non-homogeneous polynomials $\rightarrow$ homogeneous components of highest degree

❑ Existence of semi-regular sequence is open (Fröberg's conjecture)

- ☞ Finding one explicit example

Complexity of computing a Gröbner basis – II

Macaulay matrix $\mathcal{M}^{\text{acaulay}}_{D,m}$ of degree D

- ☞ Regularity $\approx$ algebraic independence of Macaulay matrices
- ☞ Trivial syzygies $p_i p_j = p_j p_i$.

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

Complexity of computing a Gröbner basis – II

- Let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a regular sequence ($n \leqslant m$).

$$D_{\mathrm{reg}} = \frac{\sum_{i=1}^{m}(d_i - 1) + 1}{2}.$$

  - $D_{\mathrm{reg}} = (n+1)$ for $n = m$ quadratic polynomials.
- Let $p_1, \ldots, p_n, p_{n+1} \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a semi-regular sequence.

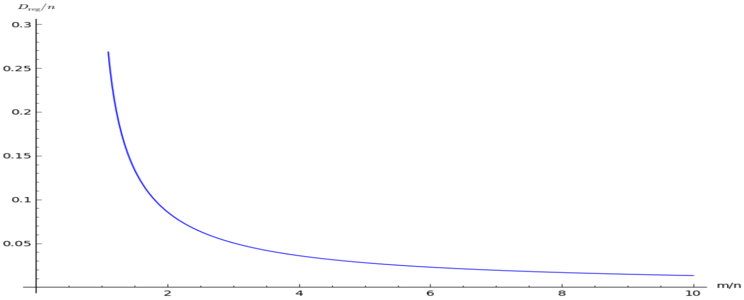
$$D_{\mathrm{reg}} = (n+1)/2.$$

Complexity of computing a Gröbner basis – II

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 :

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



Complexity of computing a Gröbner basis – II

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 if $m = \binom{n+1}{2}$
- ☞ sub-exponential complexity if $m = \tilde{O}(n)$
- ☞ exponential complexity if $m = O(n)$ or $m = n + \mathrm{Cst}$

Hybrid approach for solving $\texttt{PoSSo}_q$

$\texttt{PoSSo}_q$

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

$$p_1(z_1, \ldots, z_n) = 0, \ldots, p_m(z_1, \ldots, z_n) = 0.$$

L. Bettale, J.-C. Faugère, L. P.
"Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach".
ISSAC 2012

Algorithm

For $\mathbf{a} \in \mathbb{F}_q^k$

Specialize variables

$$\tilde{\mathbf{p}} \leftarrow (\tilde{p}_1(x_1, \ldots, x_{n-k}, \mathbf{a}), \ldots, \tilde{p}_m(x_1, \ldots, x_{n-k}, \mathbf{a}))$$

$V \leftarrow V_{\mathbb{F}_q}(\tilde{\mathbf{p}})$ $\boxed{\textbf{Solve the sub-systems}}$

If $V \neq \emptyset$ then return $\left\{(v, \mathbf{a}) \in \mathbb{F}_q^{n-k} \times \mathbb{F}_q^k | v \in V\right\}$.

Hybrid approach for solving $\texttt{PoSSo}_q$

Algorithm

For $\mathbf{a} \in \mathbb{F}_q^k$

Specialize variables

$$\tilde{\mathbf{p}} \leftarrow (\tilde{p}_1(x_1, \ldots, x_{n-k}, \mathbf{a}), \ldots, \tilde{p}_m(x_1, \ldots, x_{n-k}, \mathbf{a}))$$

$V \leftarrow V_{\mathbb{F}_q}(\tilde{\mathbf{p}})$ $\boxed{\textbf{Solve the sub-systems}}$

If $V \neq \emptyset$ then return $\left\{(v, \mathbf{a}) \in \mathbb{F}_q^{n-k} \times \mathbb{F}_q^k | v \in V\right\}$.

Intuition

- $D_{\mathrm{reg}} = (n+1)$ for $m = n$ quadratic polynomials.
- $D_{\mathrm{reg}} = (n+1)/2$ for $m = n+1$ quadratic polynomials.

Hybrid approach for solving $\texttt{PoSSo}_q$

Algorithm

For $\mathbf{a} \in \mathbb{F}_q^k$

Specialize variables

$$\tilde{\mathbf{p}} \leftarrow (\tilde{p}_1(x_1, \ldots, x_{n-k}, \mathbf{a}), \ldots, \tilde{p}_m(x_1, \ldots, x_{n-k}, \mathbf{a}))$$

$V \leftarrow V_{\mathbb{F}_q}(\tilde{\mathbf{p}})$ $\boxed{\textbf{Solve} \text{ the sub-systems}}$

If $V \neq \emptyset$ then return $\left\{(v, \mathbf{a}) \in \mathbb{F}_q^{n-k} \times \mathbb{F}_q^k | v \in V\right\}$.

Complexity

Assuming semi-regularity of the sub-systems, the asymptotic complexity is:

$$O\left(2^{\left(1.38 - 0.63\omega \; \log_2(q)^{-1}\right) n \cdot \omega}\right), \text{with } 2 \leqslant \omega \leqslant 3 \text{ and } \log(q) \ll n.$$

Asymptotic gain : $O(2^{0.62\omega n})$.

Outline

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:

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

Hardness Results

- ✔ Solving BinaryErrorLWE with $m = n\left(1 + \Omega(1/log(n))\right)$ allows to solve Gap-SVP in the worst-case
- ☞ Polynomial-time algorithm if $m = O(n^2)$

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**.

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

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

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

Until Now

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

Arora-Ge Modelling

Solving `BinaryErrorLWE` $\equiv$

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

Arora-Ge Algorithm

`BinaryErrorLWE`: m quadratic equations in n variables over $\mathbb{F}_q$.

✔ $\boxed{\textbf{Linearisation}}$ $\mapsto$ polynomial-time algo. when $m = O(n^2)$.

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.

Solving `BinaryErrorLWE` with Gröbner Bases

Asymptotic Expansion

Let $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ 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 $\mathcal{O}\left(2^{\frac{3n \log \log \log n}{8 \log \log n}}\right)$.

Outline

Boolean Polynomial System Solving ($\texttt{PoSSo}_2$)

$\texttt{PoSSo}_2$

Input. quadratic polynomials $p_1, \ldots, p_m \in \mathbb{F}_2[x_1, \ldots, x_n]$
Question. Find – if any – $(z_1, \ldots, z_n) \in \mathbb{F}_2^n$ such that:

$$p_1(z_1, \ldots, z_n) = 0, \ldots, p_m(z_1, \ldots, z_n) = 0$$

- ❑ $\texttt{PoSSo}_2$ remains NP-hard

Solving $\texttt{PoSSo}_2$ – Classical setting

- ☛ Optimized exhaustive search in $4 \log_2 2^n$ [C. Bouillaguet, C.-Mou Cheng, T. Chou, R. Niederhagen, B-Y. Yang, SAC, 2013]
- ☛ BooleanSolve $O(2^{0.792n})$ [M. Bardet, J.-C. Faugère, B. Salvy, P-J. Spaenlehauer, JoC, 2013], regularity assumption on the input
- ☛ Polynomial approximation, $O^*(2^{0.6943\,n})$ [I. Dinur, SODA, 2021], no assumption

Boolean Polynomial System Solving ($\texttt{PoSSo}_2$)

Overview

- $F : \{0,1\}^n \to \{0,1\}$
- Find $\mathbf{x}^* \in \{0,1\}^n$ such that $F(\mathbf{x}^*) = 1$
- Complexity $\left\lceil \frac{\pi}{4}\sqrt{\frac{2^n}{|f^{-1}(1)|}} \right\rceil$ evaluations of F as a quantum circuit

[Schwabe-Westerbaan, SPACE, 2016]

☞ Given $\mathbf{p} = (p_1, \ldots, p_m) \in \mathbb{F}_2[x_1, \ldots, x_n]^m$, F is the function that returns 1 if $\mathbf{p}(\mathbf{x}^*) = \mathbf{0}$.

Boolean Polynomial System Solving (PoSSo_2)

Solving PoSSo_2 – Quantum setting

- Quantum exhaustive search in $O(2^{n/2}mn^2)$ [Schwabe-Westerbaan, SPACE, 2016]
- Reduction to quantum linear system solving (HHL) [Chen-Gao, Journal of Systems Science and Complexity, 2018]

  Solving PoSSo_2 with probability $\geqslant 1-\epsilon$ in:

$$\tilde{O}\big(\mathrm{poly}(n)\kappa^2 \log(1/\epsilon)\big),$$

  κ *condition number* of a certain (Macaulay) matrix.

  - Condition number κ is exponential in the hamming weight of the solution [Ding-Gheorghiu-Gilyén-Hallgren-Li, ArXiv, 2021]

Algorithms beating the quadratic speed-up ?

Key Ideas – BooleanSolve

1/ Combine exhaustive search and Gröbner basis-like computation

L. Bettale, J.-C. Faugère and L. P.
"*Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach*".
ISSAC '12.

M. Bardet, J.-C. Faugère, B. Salvy, P.-J. Spaenlehauer.
"*On the Complexity of Solving Quadratic Boolean Systems*".
J. Complexity, 2013.

BooleanSolve ($k < n$)

For $\mathbf{a} \in \mathbb{F}_2^k$

$\tilde{\mathbf{p}}_{\mathbf{a}} \leftarrow (p_1(x_1, \ldots, x_{n-k}, \mathbf{a}), \ldots, p_m(x_1, \ldots, x_{n-k}, \mathbf{a}))$

If $\tilde{\mathbf{p}}_{\mathbf{a}}$ is **consistent**

☞ **Linear algebra** computation with $\omega = 2$ (Las-Vegas variant)

Find $\tilde{\mathbf{z}} = (\tilde{z}_1, \ldots, \tilde{z}_{n-k}) \in \mathbb{F}_2^{n-k}$ such that

$$\tilde{\mathbf{p}}_{\mathbf{a}}(\tilde{\mathbf{z}}) = \mathbf{p}(\mathbf{a}, \tilde{\mathbf{z}}) = \mathbf{0}.$$

☞ Exhaustive search for the remaining variables

Key Ideas – BooleanSolve

2/ Checking consistency with linear algebra

Hilbert's Nullstallensatz

Let $p_1, \ldots, p_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ and $\mathbf{M} = \mathcal{M}_{D,m}^{\mathrm{acaulay}}$ be the corresponding Boolean Macaulay matrix for a large enough degree D. It holds that the **linear system**

$$\mathbf{u} \cdot \mathbf{M} = (0, 0, \ldots, 0, 1) \text{ has a solution}$$

$\Leftrightarrow$ **non-linear system** $p_1 = 0, \ldots, p_m = 0$ has no solution in $\mathbb{F}_2^n$.

Key Ideas – BooleanSolve

M. Giesbrecht , A. Lobo and B. D. Saunders.
"*Certifying Inconsistency of Sparse Linear Systems*".
ISSAC, 1997.

GLS algorithm – Complexity (Las-Vegas)

It checks the consistency of an $N \times N$ matrix over $\mathbb{F}_q$ with :

- $O(N \log N)$ evaluations of black-boxes and
- additional $O(N^2 \log^2 N \log \log N)$ operations.

☞ Proven fast linear algebra in quadratic-time

QuantumBooleanSolve

BooleanSolve ($k < n$)

For $\mathbf{a} \in \mathbb{F}_2^k$

- $\tilde{\mathbf{p}}_{\mathbf{a}} \leftarrow (\tilde{p}_1(x_1, \ldots, x_{n-k}, \mathbf{a}), \ldots, \tilde{p}_m(x_1, \ldots, x_{n-k}, \mathbf{a}))$
- If $\tilde{\mathbf{p}}_{\mathbf{a}}$ is **consistent**

☞ **Linear algebra** computation with $\omega = 2$ (Las-Vegas variant)

- Find $\tilde{\mathbf{z}} = (\tilde{z}_1, \ldots, \tilde{z}_{n-k}) \in \mathbb{F}_2^{n-k}$ such that

$$\tilde{\mathbf{p}}_{\mathbf{a}}(\tilde{\mathbf{z}}) = \mathbf{p}(\mathbf{a}, \tilde{\mathbf{z}}) = \mathbf{0}.$$

☞ Exhaustive search for the remaining variables

QuantumBooleanSolve ($k < n$)

- Find $\mathbf{a} \in \mathbb{F}_2^k$ such that $\tilde{\mathbf{p}}_{\mathbf{a}}$ is **consistent** with a Grover-like search
  - ☞ Quantum circuit for Giesbrecht-Lobo-Saunders algorithm
- Find $\tilde{\mathbf{z}} = (\tilde{z}_1, \ldots, \tilde{z}_{n-k}) \in \mathbb{F}_2^{n-k}$ such that $\tilde{\mathbf{p}}_{\mathbf{a}}(\tilde{\mathbf{z}}) = \mathbf{p}(\mathbf{a}, \tilde{\mathbf{z}}) = \mathbf{0}$ with Schwabe-Westerbaan quantum exhaustive search

QuantumBooleanSolve

QuantumBooleanSolve ($k < n$)

- Find $\mathbf{a} \in \mathbb{F}_2^k$ such that $\tilde{\mathbf{p}}_\mathbf{a}$ is **consistent** with a Grover-like search
  - ☞ Quantum circuit for Giesbrecht-Lobo-Saunders algorithm
- Find $\tilde{\mathbf{z}} = (\tilde{z}_1, \ldots, \tilde{z}_{n-k}) \in \mathbb{F}_2^{n-k}$ such that $\tilde{\mathbf{p}}_\mathbf{a}(\tilde{\mathbf{z}}) = \mathbf{p}(\mathbf{a}, \tilde{\mathbf{z}}) = \mathbf{0}$ with Schwabe-Westerbaan quantum exhaustive search

Complexity ($m = n, k = \gamma n$)

Under a **regularity assumption**, QuantumBooleanSolve has complexity :

$$O(2^{\frac{k}{2}} \times (2^{2F_\alpha(\gamma)+\epsilon)n}) = O(2^{(\frac{1-\gamma}{2}+2F_\alpha(\gamma)+\epsilon)n}),$$

where $\gamma = 1 - \frac{k}{n}$, $F_\alpha(\gamma) = -\gamma \log_2(D^D(1-D)^{(1-D)})$ with $D = M(\frac{1}{\gamma})$, and

$$M(x) = -x + \frac{1}{2} + \frac{1}{2}\sqrt{2x^2 - 10x - 1 + 2(x+2)\sqrt{x(x+2)}}.$$

QuantumBooleanSolve

Complexity ($m = n, k = \gamma n$)

Under a **regularity assumption**, QuantumBooleanSolve has complexity :

$$O(2^{\frac{k}{2}} \times (2^{2F_\alpha(\gamma)+\epsilon)n}) = O(2^{(\frac{1-\gamma}{2}+2F_\alpha(\gamma)+\epsilon)n}),$$

where $\gamma = 1 - \frac{k}{n}$, $F_\alpha(\gamma) = -\gamma \log_2(D^D(1-D)^{(1-D)})$ with $D = M(\frac{1}{\gamma})$, and

$$M(x) = -x + \frac{1}{2} + \frac{1}{2}\sqrt{2x^2 - 10x - 1 + 2(x+2)\sqrt{x(x+2)}}.$$

BooleanSolve

- ☞ $\boxed{O(2^{0.462\,n}) \text{ for solving } \mathtt{PoSSo}_2}$
- ☞ Square root of $O(2^{n \cdot \frac{0.792}{2}}) = O(2^{0.396n})$

QuantumMQSolve

$\boxed{\text{Generalization for any } q > 3}$

Complexity $(m = n, k = \gamma n)$

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p), \text{ and}$$
$$M^q(x) = x - \tfrac{1}{2} - \sqrt{x(x-1)}.$$
$$F^q_\alpha(\gamma) = \left(\gamma + M^q(\alpha/\gamma)\right) H\left(\tfrac{\gamma}{\gamma + M^q(1/\gamma)}\right).$$

For any $\epsilon > 0$, QuantumMQSolve has expected complexity:

$$O(2^{(\log_2(q)\frac{1-\gamma}{2} + 2F^q_\alpha(\gamma) + \epsilon)n}).$$

The asymptotic complexity is:

$$O\left(2^{\left(2.76 - 2.48\log_2(q)^{-1}\right)n}\right), \text{ assuming } \log(q) \ll n.$$