Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra

Alessio Caminata (Universitat de Barcelona)

joint work with Elisa Gorla

PQCrypto 2017
Utrecht, 26–28 June 2017

Algebraic attack with Gröbner bases

- Multivariate cryptosystem

$$\mathbb{F}_q^n \ni \underline{x} = (x_1, \ldots, x_n) \mapsto (y_1, \ldots, y_r) := (p_1(\underline{x}), \ldots, p_r(\underline{x})) \in \mathbb{F}_q^r$$

- One can try to break it with an *algebraic attack*, i.e. by computing a Gröbner basis of the associated ideal $I = (f_1, \ldots, f_r)$, where $f_i := y_i - p_i$.
- Currently fastest algorithms to compute a Gröbner basis (F_4/F_5) have complexity

$$O\left(m\binom{n+s-1}{s}^{\omega-1}\right)$$

where $m = \sum_{i=1}^{r}\binom{n+s-d_i-1}{s-d_i}$, $\omega \in [2,3]$, $d_i = \deg f_i$, and $s = \text{solv. deg}(I)$ is the solving degree of I, i.e. the highest degree of polynomials involved in the computation of the Gröbner basis.

Solving degree and Castelnuovo-Mumford regularity

In order to design a multivariate cryptosystem that is secure against algebraic attacks, one needs to know how the solving degree depends on the parameters of the system.

Theorem (C.-Gorla)

Let $\mathbb{F}$ be a field, let $R := \mathbb{F}[x_1, \ldots, x_n]$, and let $I := (f_1, \ldots, f_r)$ be an ideal of R. Assume that $\tilde{I} := (f_1^h, \ldots, f_r^h)$ is in generic coordinates in $\overline{\mathbb{F}}[x_1, \ldots, x_n, t]$, where f_i^h is the homogenization of f_i, then

$$\text{solv. deg}_{DRL}(I) \leq \text{reg}(\tilde{I})$$

and equality holds if $\mathbb{F}$ has characteristics zero.

Here $\text{reg}(\tilde{I})$ is the Castelnuovo-Mumford regularity of $\tilde{I}$ and can be read from its minimal graded free resolution:

$$0 \to \bigoplus_{j\in\mathbb{Z}} R(-j)^{\beta_{p,j}} \to \cdots \to \bigoplus_{j\in\mathbb{Z}} R(-j)^{\beta_{1,j}} \xrightarrow{\varphi_1} \bigoplus_{j\in\mathbb{Z}} R(-j)^{\beta_{0,j}} \xrightarrow{\varphi_0} \tilde{I} \to 0$$

It is $\text{reg}(I) := \max\{j - i : \ \beta_{i,j} \neq 0\}$.

Applications

Use knowledge on the regularity from commutative algebra to produce bounds for the solving degree.

1. **Zero-dimensional ideals.** Let $I := (f_1, \ldots, f_r) \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an ideal generated in degree at most d. Assume that $\tilde{I} := (f_1^h, \ldots, f_r^h)$ is in generic coordinates and its projective zero-locus over $\overline{\mathbb{F}}$ consists of a finite number of points, then

$$\text{solv. deg}_{DRL}(I) \leq (n+1)(d-1)+1.$$

2. **MinRank Problem.** Let M be an $m \times n$ matrix with $m \leq n$ whose entries are *sufficiently general* linear forms in a polynomial ring over a field. Then the solving degree of the corresponding MinRank Problem is

$$\text{solv. deg}_{DRL}\, I_m(M) \leq m.$$

Thank you!!

Questions?

Essential bibliography

D.J. Bernstein, J. Buchmann, E. Dahmen,
Post-Quantum Cryptography, Springer Verlag, 2009

A. Caminata, E. Gorla,
Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra, preprint 2017.

J.C. Faugère,
A new efficient algorithm for computing Gröbner bases (F4), Journal of Pure and Applied Algebra, vol. 139, pp. 61–88, 1999.