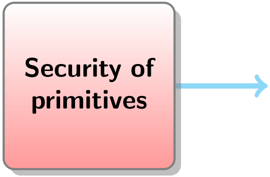
Algebraic cryptanalysis: how Gröbner bases techniques can be used in cryptanalysis

Magali Bardet

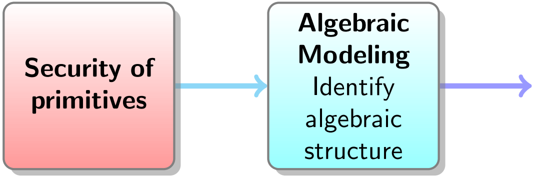
LITIS, University of Rouen Normandie, France
magali.bardet@univ-rouen.fr

STAP 2023,
April 23rd, 2023

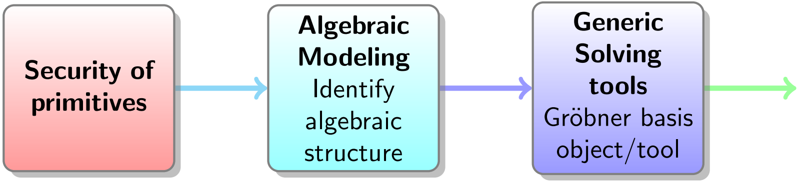
Algebraic Cryptanalysis



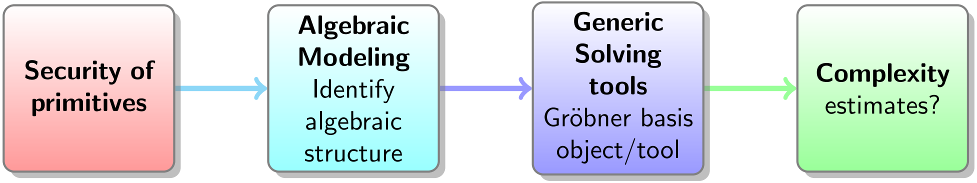
Algebraic Cryptanalysis



Algebraic Cryptanalysis



Algebraic Cryptanalysis



Algebraic Cryptanalysis can be devastating

Famous practical cryptanalyses in $\simeq$ **2 days**:

- attacking first HFE Challenge (80 bits) (J.-C. Faugère and Joux 2003)
- attacking finalist Rainbow (128 bits) (Beullens 2022)

Many other examples in the literature.

Algebraic Modeling

Principle: write a Polynomial System

$$\begin{cases} f_1(x_1,\dots,x_n) \\ \vdots \\ f_m(x_1,\dots,x_n) \end{cases}, \quad \deg(f_i)=d_i, f_i \in \mathbb{K}[x_1,\dots,x_n].$$

such that finding the set of solutions

$$V(f_1,\dots,f_m) = \{(x_1,\dots,x_n) \in \overline{\mathbb{K}}^n : f_i(x_1,\dots,x_n)=0, \forall i \in \{1..m\}\}$$

gives (part of) the secret.

Ideally: *any* solution is related to the secret!

Algebraic Modeling

Principle: write a Polynomial System

$$\begin{cases} f_1(x_1,\ldots,x_n) \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1,\ldots,x_n].$$

such that finding the set of solutions

$$V(f_1,\ldots,f_m) = \left\{(x_1,\ldots,x_n) \in \overline{\mathbb{K}}^n : f_i(x_1,\ldots,x_n) = 0, \forall i \in \{1..m\}\right\}$$

gives (part of) the secret.

Ideally: *any* solution is related to the secret!

- Otherwise, we have to deal with spurious solutions.

Algebraic Modeling

Principle: write a Polynomial System

$$\begin{cases} f_1(x_1,\dots,x_n) \\ \vdots \\ f_m(x_1,\dots,x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1,\dots,x_n].$$

such that finding the set of solutions

$$V(f_1,\dots,f_m) = \{(x_1,\dots,x_n) \in \overline{\mathbb{K}}^n : f_i(x_1,\dots,x_n) = 0, \forall i \in \{1..m\}\}$$

gives (part of) the secret.

Ideally: *any* solution is related to the secret!

- Otherwise, we have to deal with spurious solutions.
- Solutions in $\mathbb{F}_q$: algebraic constraint! add the field equations $x_i^q - x_i$.

Solving the algebraic system using Gröbner bases (object)

- A particular basis of the ideal

$$I(f_1, \ldots, f_m) = \langle f_1, \ldots, f_m \rangle$$

  that solves the ideal-membership problem.
- Depends on the choice of a monomial ordering.

Solving the algebraic system using Gröbner bases (object)

- A particular basis of the ideal

$$I(f_1, \ldots, f_m) = \langle f_1, \ldots, f_m \rangle$$

  that solves the ideal-membership problem.
- Depends on the choice of a monomial ordering.

A hard problem

- Ideal Membership testing is EXPSPACE-complete,
- Existence of solutions to a system of polynomial equations over a finite field is NP-complete (Fraenkel and Yesha 1979),

Gröbner basis algorithms

General algorithms, for any input system:

- Buchberger (Buchberger 1965),
- F4 (J.-C. Faugère 1999),
- F5 (J.-C. Faugère 2002).

The algorithms will always terminate and give the Gröbner basis.
But the time is hard to predict for *any* instance.

Gröbner basis algorithms

General algorithms, for any input system:

- Buchberger (Buchberger 1965),
- F4 (J.-C. Faugère 1999),
- F5 (J.-C. Faugère 2002).

The algorithms will always terminate and give the Gröbner basis.
But the time is hard to predict for *any* instance.

Specific algorithms, for a particular class of systems:

The algorithms will terminate in a predictable time.
The result is not always a Gröbner basis of the system.
For random instances in the specific class, the result is a Gröbner basis.

Properties of monomial orderings

Different monomial orderings have different properties

- the *lex* order (Lexicographical): in Shape Position, for a zero-dimension ideal, the lex basis is

$$\begin{cases} x_1 - g_1(x_n), \\ \vdots \\ x_{n-1} - g_{n-1}(x_n), \\ g_n(x_n), \end{cases}$$

  with $\deg(g_n) = D$ the number of solutions to the system.
- the *grevlex* order (Graded Reverse Lexicographical): usually the best one w.r.t. the complexity.
- the *elim* order (Elimination): two blocks of variables $\mathbf{x} > \mathbf{y}$.

Monomial ordering examples

Lexicographical ordering $x_1 > \cdots > x_n$

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} > x_1^{\beta_1} \ldots x_n^{\beta_n} \text{ iff } \begin{cases} \alpha_j = \beta_j & \forall j < i, \\ \alpha_i > \beta_i. \end{cases}$$

Graded Reverse Lexicographical ordering $x_1 > \cdots > x_n$

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} > x_1^{\beta_1} \ldots x_n^{\beta_n} \text{ iff } \begin{cases} \alpha_j = \beta_j & \forall j > i, \\ \alpha_i < \beta_i. \end{cases}$$

Elimination Ordering $\mathbf{x} > \mathbf{y}$

$$\mathbf{x}^{\alpha}\mathbf{y}^{\beta} > \mathbf{x}^{\alpha'}\mathbf{y}^{\beta'} \text{ iff } \begin{cases} \alpha >_1 \alpha' \\ \text{or } \alpha = \alpha' \text{ and } \beta >_2 \beta'. \end{cases}$$

Family of random zero-dimensional systems

Hypotheses for cryptanalysis

- the variety is zero-dimensional (otherwise, change the modeling!).
- the instances are “random” (not the system).

Change of ordering FGLM for zero-dimensional systems

- The FGLM (J.-C. Faugère, Gianni, Lazard, and Mora 1993) Algorithm performs a change of ordering in complexity

$$O(nD^3),$$

n number of variables, $n \to \infty$, D degree of the ideal (number of solutions).

Change of ordering FGLM for zero-dimensional systems

- The FGLM (J.-C. Faugère, Gianni, Lazard, and Mora 1993) Algorithm performs a change of ordering in complexity

$$O(nD^3),$$

n number of variables, $n \to \infty$, D degree of the ideal (number of solutions).

- Complexity for grevlex to lex (Shape position) (J.-C. Faugère, Gaudry, Huot, and Renault 2014):

$$O(\log_2(D)(D^\omega + n\log_2(D)D)).$$

Change of ordering FGLM for zero-dimensional systems

- The FGLM (J.-C. Faugère, Gianni, Lazard, and Mora 1993) Algorithm performs a change of ordering in complexity

$$O(nD^3),$$

n number of variables, $n \to \infty$, D degree of the ideal (number of solutions).

- Complexity for grevlex to lex (Shape position) (J.-C. Faugère, Gaudry, Huot, and Renault 2014):

$$O(\log_2(D)(D^\omega + n\log_2(D)D)).$$

- Sparse versions for generic systems grevlex to lex (J.-C. Faugère and Mou 2017) in

$$O\left(\sqrt{\frac{6}{n\pi}}D^{2+\frac{n-1}{n}}\right).$$

Systems with 0 or 1 solution

The grevlex and lex bases are the same:

- If the system has 1 solution:

$$\begin{cases} x_1 - a_1, \\ \vdots \\ x_n - a_n, \end{cases}$$

  where $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$ is the solution.
- If the system has no solution:

$$\langle 1 \rangle.$$

Adding the field equations

Should I add the field equations to the system?

- Does the ideal have solutions in the algebraic closure of $\mathbb{F}_q$? How many?
- Is the maximal degree D reached during the computation smaller than q?
- Are there solutions in $\overline{\mathbb{F}_q}$ that I'm not interested in?

Adding the field equations

Should I add the field equations to the system?

- Does the ideal have solutions in the algebraic closure of $\mathbb{F}_q$? How many?
- Is the maximal degree D reached during the computation smaller than q?
- Are there solutions in $\overline{\mathbb{F}_q}$ that I'm not interested in?

When should I add the field equations?

- from the beginning,
- to the lex basis (gcd).

Complexity of computing a Gröbner basis

- worst case: doubly exponential! polynomials of degree d^{2^n} in the basis, any monomial ordering (Mayr and Meyer 1982).
- zero-dimensional, grevlex: simply exponential (Lazard 1983; Giusti 1984).
- relation to linear algebra for the computation: Macaulay matrices.

Tools from computer algebra toward complexity analysis

$$\text{System} \begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1, \ldots, x_n].$$

- Macaulay Matrices (Macaulay 1902):

$$\mathcal{M}_d(\{f_1, \ldots, f_m\}) = \begin{matrix} \vdots \\ (t, i) \\ \vdots \end{matrix} \overset{t'}{\begin{pmatrix} & & \\ & \text{coeff}(tf_i, t') & \\ & & \end{pmatrix}}$$

Tools from computer algebra toward complexity analysis

$$\text{System} \begin{cases} f_1(x_1,\dots,x_n) \\ \vdots \\ f_m(x_1,\dots,x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1,\dots,x_n].$$

- Macaulay Matrices (Macaulay 1902):

$$\mathscr{M}_d(\{f_1,\dots,f_m\}) = \begin{matrix} \vdots \\ (t,i) \\ \vdots \end{matrix} \overset{t'}{\begin{pmatrix} & \\ & \text{coeff}(tf_i, t') \\ & \end{pmatrix}}$$

- Describes the vector space $\langle tf_i : \deg(tf_i) = d \rangle_{\mathbb{K}}$.

Tools from computer algebra toward complexity analysis

$$\text{System} \begin{cases} f_1(x_1,\ldots,x_n) \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1,\ldots,x_n].$$

- Macaulay Matrices (Macaulay 1902):

$$\mathscr{M}_d(\{f_1,\ldots,f_m\}) = \begin{matrix} \vdots \\ (t,i) \\ \vdots \end{matrix} \overset{t'}{\begin{pmatrix} & \\ & \text{coeff}(tf_i, t') \\ & \end{pmatrix}}$$

- Describes the vector space $\langle tf_i : \deg(tf_i) = d \rangle_{\mathbb{K}}$.
- Linear algebra on the Macaulay matrices up to degree D computes a Gröbner basis (Lazard 1983,Giusti 1984).

Complexity bounds

Linear algebra on the Macaulay matrix of degree D

A Gröbner basis of a system $(f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]$ up to degree D for a graded monomial ordering can be computed in, at most,

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right) \qquad n, m \to \infty.$$

operations.

Complexity bounds

Linear algebra on the Macaulay matrix of degree D

A Gröbner basis of a system $(f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]$ up to degree D for a graded monomial ordering can be computed in, at most,

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right) \qquad n, m \to \infty.$$

operations.

Main challenges

- Estimate D.
- Identify unnecessary computations to reduce the complexity, e.g. to $O\left(\binom{n+D}{D}^{\omega}\right)$.
- If there are fall degree at degree $< D$, construct a better strategy (algorithm) to take that into account, and estimate its complexity.

Generic Complexity analysis

Known classes of particular systems (not exhaustive)

- **regular** systems (Macaulay 1916), $\#$ eq $\leqslant \#$ vars,
- **determinantal** systems (Conca and Herzog 1994),
- **semi-regular** systems (Bardet, J.-C. Faugère, and Salvy 2004), $\#$ eq $\geqslant \#$ vars,
- solutions in $\mathbb{F}_2$: **boolean semi-regular** systems (Bardet, J.-C. Faugère, Salvy, and Yang 2005),
- **bi-regular bilinear** systems (J.-C. Faugère, Safey El Din, and P.-J. Spaenlehauer 2011).

Difference between classes

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right) \qquad\qquad n,m\rightarrow\infty.$$

Examples of quadratic equations:

- $m=n$ regular system: : $D\leqslant n+1$,
- $m=n+1$ semi-regular system: $D\leqslant\lceil\frac{n+2}{2}\rceil$,
- $m=n$ regular bilinear system with $\lfloor\frac{n}{2}\rfloor$ variables x and $\lceil\frac{n}{2}\rceil$ variables y: $D\leqslant\lceil\frac{n}{2}\rceil$.
- $m=n$ regular over $\mathbb{F}_2$: $D\simeq\frac{n}{11}$, $O(\binom{n}{D}^{\omega})$

Algebraic attack

For each class we know

- relations between rows in the Macaulay matrices,
- the rank of the Macaulay matrices for generic systems,
- the maximal degree $D \rightarrow$ complexity estimates,
- a specific Gb algorithm that is more efficient.

Algebraic attack

For each class we know

- relations between rows in the Macaulay matrices,
- the rank of the Macaulay matrices for generic systems,
- the maximal degree $D \rightarrow$ complexity estimates,
- a specific Gb algorithm that is more efficient.

If the system is not in a known class

- Identify a generic behavior,
- Identify a specific algorithm to compute the Gb,
- Create a new class!

Homogeneous vs Affine

- All bounds are given for homogeneous polynomials.

Homogeneous vs Affine

- All bounds are given for homogeneous polynomials.
- For affine systems: the same complexity if no fall degree before degree D, the complexity is then the cost of reducing several matrices at degree D (sometimes $D+1$, at most $2D-1$).

Homogeneous vs Affine

- All bounds are given for homogeneous polynomials.
- For affine systems: the same complexity if no fall degree before degree D, the complexity is then the cost of reducing several matrices at degree D (sometimes $D+1$, at most $2D-1$).
- In this case, D is the *first fall degree*, also the *solving degree* and the *degree of regularity* and is related to the complexity.

Homogeneous vs Affine

- All bounds are given for homogeneous polynomials.
- For affine systems: the same complexity if no fall degree before degree D, the complexity is then the cost of reducing several matrices at degree D (sometimes $D+1$, at most $2D-1$).
- In this case, D is the *first fall degree*, also the *solving degree* and the *degree of regularity* and is related to the complexity.
- Otherwise, first fall degree is not related to complexity estimates!

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\operatorname{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r.$$

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\mathrm{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r.$$

- NP-complete problem (Buss, Frandsen, Shallit 1999),

The MinRank Problem

- Input: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- Output: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r.$$

- NP-complete problem (Buss, Frandsen, Shallit 1999),
- used to cryptanalyse various multivariate and code-based cryptosystems.

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r.$$

- NP-complete problem (Buss, Frandsen, Shallit 1999),
- used to cryptanalyse various multivariate and code-based cryptosystems.
- This is exactly the decoding problem for matrix codes,

The MinRank Problem

- Input: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- Output: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\operatorname{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r.$$

- NP-complete problem (Buss, Frandsen, Shallit 1999),
- used to cryptanalyse various multivariate and code-based cryptosystems.
- This is exactly the decoding problem for matrix codes,
- $K < (m-r)(n-r)$: 0 or 1 solution *in the algebraic closure* of $\mathbb{F}_q$.

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r.$$

- NP-complete problem (Buss, Frandsen, Shallit 1999),
- used to cryptanalyse various multivariate and code-based cryptosystems.
- This is exactly the decoding problem for matrix codes,
- $K < (m-r)(n-r)$: 0 or 1 solution *in the algebraic closure* of $\mathbb{F}_q$.
- No need to add the field equations: already in the ideal!

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \dots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \dots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\operatorname{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r.$$

- NP-complete problem (Buss, Frandsen, Shallit 1999),
- used to cryptanalyse various multivariate and code-based cryptosystems.
- This is exactly the decoding problem for matrix codes,
- $K < (m-r)(n-r)$: 0 or 1 solution *in the algebraic closure* of $\mathbb{F}_q$.
- No need to add the field equations: already in the ideal!
- For very small q (e.g. $q = 2$): adding small degree equations can speed up the computation.

MinRank problem $\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r$

- Kipnis-Shamir modeling (Kipnis and Shamir 1999)

$$\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{R} \end{pmatrix} = 0_{m\times(n-r)}, \quad \boldsymbol{R} \in \mathbb{F}_q^{r\times(n-r)}, x_i \in \mathbb{F}_q \qquad \text{(KS)}$$

MinRank problem $\mathrm{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r$

- Kipnis-Shamir modeling (Kipnis and Shamir 1999)

$$\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right)\begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{R} \end{pmatrix} = 0_{m\times(n-r)}, \quad \boldsymbol{R} \in \mathbb{F}_q^{r\times(n-r)}, x_i \in \mathbb{F}_q \qquad \text{(KS)}$$

- Minors modeling (J. Faugère, Safey El Din, and P. Spaenlehauer 2010)

$$\mathrm{Minors}_{r+1}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) = 0 \qquad \text{(Minors)}$$

MinRank problem $\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r$

- Kipnis-Shamir modeling (Kipnis and Shamir 1999)

$$\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{R} \end{pmatrix} = 0_{m\times(n-r)}, \quad \boldsymbol{R} \in \mathbb{F}_q^{r\times(n-r)}, x_i \in \mathbb{F}_q \qquad \text{(KS)}$$

- Minors modeling (J. Faugère, Safey El Din, and P. Spaenlehauer 2010)

$$\text{Minors}_{r+1}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) = 0 \qquad \text{(Minors)}$$

- Support Minors modeling, (Bardet, Bros, Cabarcas, Gaborit, et al. 2020)

$$\text{Minors}_{r+1}\begin{pmatrix} (\sum_{i=1}^{K} x_i \boldsymbol{M}_i)_{j,*} \\ \boldsymbol{R} \quad \boldsymbol{I}_r \end{pmatrix} = 0 \qquad \forall j \in \{1..m\}. \qquad \text{(SM)}$$

MinRank problem $\mathrm{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r$

- Kipnis-Shamir modeling (Kipnis and Shamir 1999)

$$\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{R} \end{pmatrix} = 0_{m\times(n-r)}, \quad \boldsymbol{R} \in \mathbb{F}_q^{r\times(n-r)}, x_i \in \mathbb{F}_q \qquad \text{(KS)}$$

- Minors modeling (J. Faugère, Safey El Din, and P. Spaenlehauer 2010)

$$\mathrm{Minors}_{r+1}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) = 0 \qquad \text{(Minors)}$$

- Support Minors modeling, (Bardet, Bros, Cabarcas, Gaborit, et al. 2020)

$$\mathrm{Minors}_{r+1}\begin{pmatrix} (\sum_{i=1}^{K} x_i \boldsymbol{M}_i)_{j,*} \\ \boldsymbol{R} \quad \boldsymbol{I}_r \end{pmatrix} = 0 \qquad \forall j \in \{1..m\}. \qquad \text{(SM)}$$

- Same ideal ! (Bardet and Bertin 2022; Guo and Ding 2022)

Specific systems

GeMSS signature scheme (Casanova, J. Faugère, Macario-Rat, Patarin, et al. 2019)

- alternate candidate (3rd Round of the NIST process) that suffered a MinRank attack (Tao, Petzoldt, and Ding 2021),
- the system has m solutions in an extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$,
- specific analysis using the particular algebraic structure (Banea, Briaud, Cabarcas, Perlner, et al. 2022).

Complexity estimate goes e.g. for GeMSS256 from 2^{272} to 2^{166} to 2^{75}!

Specific systems

GeMSS signature scheme (Casanova, J. Faugère, Macario-Rat, Patarin, et al. 2019)

- alternate candidate (3rd Round of the NIST process) that suffered a MinRank attack (Tao, Petzoldt, and Ding 2021),
- the system has m solutions in an extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$,
- specific analysis using the particular algebraic structure (Banea, Briaud, Cabarcas, Perlner, et al. 2022).

Complexity estimate goes e.g. for GeMSS256 from 2^{272} to 2^{166} to 2^{75}!

$\mathbb{F}_{q^m}$-linear codes

- the equations are not linearly independent! + a lot of linear equations.
- Bardet, Briaud, Bros, Gaborit, and Tillich 2022: specific analysis of the system.

Gröbner bases in Magma

Computer algebra system `magma`

- default strategy: compute the grevlex basis, then change to the lex basis using FGLM.
- `lex` by default, you can specify `"grevlex"` in the polynomial ring.
- grevlex basis computed using F4, with several heuristics (`SetVerbose("Faugere",2)`)
- an input parameter for HFE-like systems, to save memory and time.

Conclusion

- A powerful tool to solve problems that have an algebraic modeling,
- A lot of parameters to choose,
- Design specific algorithms for specific class of systems to be efficient,
- Already a lot of applications on arithmetization-oriented symmetric-key primitives.

Conclusion

- A powerful tool to solve problems that have an algebraic modeling,
- A lot of parameters to choose,
- Design specific algorithms for specific class of systems to be efficient,
- Already a lot of applications on arithmetization-oriented symmetric-key primitives.

A PhD position is available in Rouen, starting in fall, algebraic cryptanalysis.

- Banea, J., P. Briaud, D. Cabarcas, R. Perlner, et al. (Aug. 2022). "Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow". In: *Advances in Cryptology – CRYPTO 2022*. Ed. by Y. Dodis and T. Shrimpton. Vol. Part III. LNCS. Cham: Springer Nature Switzerland, pp. 376–405.
- Bardet, M. and M. Bertin (2022). "Improvement of Algebraic Attacks for Solving Superdetermined MinRank Instances". In: *PQCrypto*.
- Bardet, M., J.-C. Faugère, and B. Salvy (2004). "On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations". In: *ICPSS'04*. International Conference on Polynomial System Solving, November 24 - 25 - 26, Paris, France, pp. 71–75.
- Bardet, M., J.-C. Faugère, B. Salvy, and B.-Y. Yang (2005). "Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Quadratic Polynomial Systems". In: *MEGA'05*. Eighth International Symposium on Effective Methods in Algebraic Geometry, Porto Conte, Alghero, Sardinia (Italy), May 27th – June 1st, 15 p.

- Bardet, M., P. Briaud, M. Bros, P. Gaborit, and J.-P. Tillich (2022). *Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem*.
- Bardet, M., M. Bros, D. Cabarcas, P. Gaborit, et al. (2020). "Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems". In: *Advances in Cryptology – ASIACRYPT 2020*. Ed. by S. Moriai and H. Wang. Vol. 12491. LNCS. Cham: Springer International Publishing, pp. 507–536.
- Beullens, W. (2022). "Breaking Rainbow Takes a Weekend on a Laptop". In: *CRYPTO*.
- Buchberger, B. (1965). "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal". PhD thesis. Universitat Innsbruck.
- Caminata, A. and E. Gorla (2023). "Solving degree, last fall degree, and related invariants". In: *Journal of Symbolic Computation* 114, pp. 322–335.

- Casanova, A., J. Faugère, G. Macario-Rat, J. Patarin, et al. (Apr. 2019). *GeMSS: A Great Multivariate Short Signature*. Second round submission to the NIST post-quantum cryptography call.
- Conca, A. and J. Herzog (1994). “On the Hilbert function of determinantal rings and their canonical module”. In: *Proc. Amer. Math. Soc* 122, pp. 677–681.
- Faugère, J.-C. and A. Joux (2003). “Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases”. In: *CRYPTO*.
- Faugère, J.-C. (1999). “A New Efficient Algorithm for Computing Gröbner Bases (F4)”. In: *J. Pure Appl. Algebra* 139.1-3, pp. 61–88.
- — (2002). “A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero: F5”. In: *Proceedings ISSAC’02*. ACM press, pp. 75–83.
- Faugère, J.-C., P. Gaudry, L. Huot, and G. Renault (2014). “Sub-Cubic Change of Ordering for GröBner Basis: A Probabilistic Approach”. In: *ISSAC*.

- Faugère, J.-C., P. M. Gianni, D. Lazard, and T. Mora (1993). "Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering". In: *JSC*.
- Faugère, J.-C. and C. Mou (2017). "Sparse FGLM algorithms". In: *JSC*.
- Faugère, J., M. Safey El Din, and P. Spaenlehauer (2010). "Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology". In: *International Symposium on Symbolic and Algebraic Computation, ISSAC 2010, Munich, Germany, July 25-28, 2010*, pp. 257–264.
- — (2011). "Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity". In: *J. Symbolic Comput.* 46.4, pp. 406–437.
- Fraenkel, A. and Y. Yesha (1979). "Complexity of problems in games, graphs and algebraic equations". In: *Discrete Applied Mathematics* 1.1, pp. 15–30.
- Giusti, M. (1984). "Some effectivity problems in polynomial ideal theory". In: *Eurosam 84*. Ed. by J. Fitch. Vol. 174. Lecture Notes in Computer Science. Cambridge, 1984. Berlin: Springer Berlin / Heidelberg, pp. 159–171.

- Guo, H. and J. Ding (2022). “Algebraic Relation of Three MinRank Algebraic Modelings”. In: *Arithmetic of Finite Fields*. LNCS. Springer.
- Kipnis, A. and A. Shamir (1999). “Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization”. In: *Advances in Cryptology — CRYPTO' 99*. Ed. by M. Wiener. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 19–30.
- Lazard, D. (1983). “Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations”. In: *Computer algebra*.
- Macaulay, F. S. (1902). “Some Formulæ in Elimination”. In: *Proceedings of the London Mathematical Society*.
- — (1916). *The algebraic theory of modular systems*. Cambridge Mathematical Library. Revised reprint edition in 1994. Cambridge: Cambridge University Press, pp. xxxii+112.
- Mayr, E. W. and A. R. Meyer (1982). “The complexity of the word problems for commutative semigroups and polynomial ideals”. In: *Advances in Mathematics* 46.3, pp. 305–329.

Tao, C., A. Petzoldt, and J. Ding (2021). “Efficient Key Recovery for All HFE Signature Variants”. In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*. Ed. by T. Malkin and C. Peikert. Vol. 12825. Lecture Notes in Computer Science. Springer, pp. 70–93.