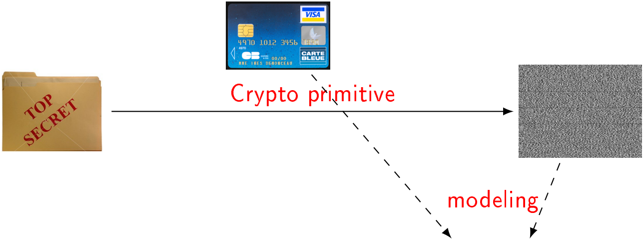
Gröbner Bases of Structured Systems and their Applications in Cryptology

Jean-Charles Faugère, Mohab Safey El Din
Pierre-Jean Spaenlehauer

UPMC – CNRS – INRIA Paris - Rocquencourt
LIP6 – SALSA team

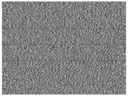
SCPQ Webinar
2012, 03/06


TOP SECRET
VISA
4970 1012 3456
CARTE BLEUE
00/00
Crypto primitive



$$\begin{aligned}
2x^2+2y^2+2z^2+2t^2+2u^2+v^2-v &= 0\\
2xy+2yz+2zt+2tu+2uv-u &= 0\\
2xz+2yt+2zu+u^2+2tv-t &= 0\\
2xt+2yu+2tu+2zv-z &= 0\\
t^2+2xv+2yv+2zv-y &= 0\\
2x+2y+2z+2t+2u+v-1 &= 0
\end{aligned}$$

Crypto primitive



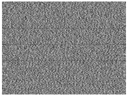
modeling

$$\begin{aligned}
2x^2+2y^2+2z^2+2t^2+2u^2+v^2-v &= 0\\
2xy+2yz+2zt+2tu+2uv-u &= 0\\
2xz+2yt+2zu+u^2+2tv-t &= 0\\
2xt+2yu+2tu+2zv-z &= 0\\
t^2+2xv+2yv+2zv-y &= 0\\
2x+2y+2z+2t+2u+v-1 &= 0
\end{aligned}$$

System solving

$$\begin{cases}
f(X_1)=0\\
f_2(X_1,X_2)=0\\
\vdots\\
f_{k_2}(X_1,X_2)=0\\
f_{k_2+1}(X_1,X_2,X_3)=0\\
\vdots\\
f_{k_{n-1}+1}(X_1,\dots,X_n)=0\\
\vdots\\
f_{k_n}(X_1,\dots,X_n)=0
\end{cases}$$

Crypto primitive



modeling

$$
\begin{aligned}
2x^2+2y^2+2z^2+2t^2+2u^2+v^2-v &= 0\\
2xy+2yz+2zt+2tu+2uv-u &= 0\\
2xz+2yt+2zu+u^2+2tv-t &= 0\\
2xt+2yu+2tu+2zv-z &= 0\\
t^2+2xv+2yv+2zv-y &= 0\\
2x+2y+2z+2t+2u+v-1 &= 0
\end{aligned}
$$

System solving

$$
\begin{cases}
f(X_1)=0\\
f_2(X_1,X_2)=0\\
\vdots\\
f_{k_2}(X_1,X_2)=0\\
f_{k_2+1}(X_1,X_2,X_3)=0\\
\vdots\\
f_{k_{n-1}+1}(X_1,\dots,X_n)=0\\
\vdots\\
f_{k_n}(X_1,\dots,X_n)=0
\end{cases}
$$

Issues

- Which **algebraic modeling** ?
- Tradeoff between the **degree** of the equations/number of **variables** ?
- Solving tools: **Gröbner bases** ? **SAT-solvers** ? ...
- **Structure** ?

Where does the structure come from ?

Where does the structure come from ?

- **Non-linearity $\rightarrow$ Security**
  - $\rightsquigarrow$ Sometimes bi(or multi)-linear
    (e.g. AES S-boxes: $x \cdot y - 1 = 0$ for $x \neq 0$).

Where does the structure come from ?

- **Non-linearity $\rightarrow$ Security**
  - $\rightsquigarrow$ Sometimes bi(or multi)-linear (e.g. AES S-boxes: $x \cdot y - 1 = 0$ for $x \neq 0$).
- **Asymmetric encryption/signature:**
  - $\rightsquigarrow$ trapdoor (e.g. HFE, Multi-HFE, McEliece).
  - $\rightsquigarrow$ Reducing the key sizes is a common issue $\rightarrow$ potential **weaknesses** due to the structure.

Motivations: Algebraic Structures in Cryptology

Where does the structure come from ?

- **Non-linearity $\rightarrow$ Security**
  - $\rightsquigarrow$ Sometimes bi(or multi)-linear (e.g. AES S-boxes: $x \cdot y - 1 = 0$ for $x \neq 0$).
- **Asymmetric encryption/signature:**
  - $\rightsquigarrow$ trapdoor (e.g. HFE, Multi-HFE, McEliece).
  - $\rightsquigarrow$ Reducing the key sizes is a common issue $\rightarrow$ potential **weaknesses** due to the structure.
- **Symmetries, invariants:**
  - $\rightsquigarrow$ **invariance of the solutions** under some transformations (e.g. MinRank).
- ...

Where does the structure come from ?

- **Non-linearity $\rightarrow$ Security**
  - $\rightsquigarrow$ Sometimes bi(or multi)-linear
    (e.g. AES S-boxes: $x \cdot y - 1 = 0$ for $x \neq 0$).
- **Asymmetric encryption/signature:**
  - $\rightsquigarrow$ trapdoor (e.g. HFE, Multi-HFE, McEliece).
  - $\rightsquigarrow$ Reducing the key sizes is a common issue
    $\rightarrow$ potential **weaknesses** due to the structure.
- **Symmetries, invariants:**
  - $\rightsquigarrow$ **invariance of the solutions** under some transformations (e.g. MinRank).
- ...

Impact on the solving process ?

Motivations: Algebraic Structures in Cryptology

Where does the structure come from ?

- **Non-linearity $\rightarrow$ Security**
  - $\rightsquigarrow$ Sometimes bi(or multi)-linear (e.g. AES S-boxes: $x \cdot y - 1 = 0$ for $x \neq 0$).
- **Asymmetric encryption/signature:**
  - $\rightsquigarrow$ trapdoor (e.g. HFE, Multi-HFE, McEliece).
  - $\rightsquigarrow$ Reducing the key sizes is a common issue $\rightarrow$ potential **weaknesses** due to the structure.
- **Symmetries, invariants:**
  - $\rightsquigarrow$ **invariance of the solutions** under some transformations (e.g. MinRank).
- ...

Impact on the solving process ?
Complexity ? Dedicated algorithms ?

Families of structured algebraic systems

Multi-homogeneous systems

- McEliece PKC.
- MinRank authentication scheme.
- ...

Families of structured algebraic systems

Multi-homogeneous systems

- McEliece PKC.
- MinRank authentication scheme.
- ...

Determinantal systems

- MinRank authentication scheme.
- Cryptosystems based on rank metric codes.
- Hidden Field Equations and variants.
- ...

Families of structured algebraic systems

Multi-homogeneous systems

- McEliece PKC.
- MinRank authentication scheme.
- ...

Determinantal systems

- MinRank authentication scheme.
- Cryptosystems based on rank metric codes.
- Hidden Field Equations and variants.
- ...

Systems invariant by symmetries

Discrete log on elliptic and hyperelliptic curves.

Outline

1. Polynomial System Solving using Gröbner Bases
2. Bilinear Systems and Application to McEliece
3. Determinantal Systems and Applications to MinRank and HFE

Gröbner bases

$\mathcal{I}$ a **polynomial ideal**. Gröbner basis (w.r.t. a monomial ordering): $G \subset \mathcal{I}$ a finite set of polynomials such that $\mathsf{LM}(\mathcal{I}) = \langle \mathsf{LM}(G) \rangle$.

- **Buchberger** [*Buchberger* Ph.D. 65].
- **$\mathbf{F_4}$** [*Faugère* J. of Pure and Appl. Alg. 99].
- **$\mathbf{F_5}$** [*Faugère* ISSAC'02].
- **FGLM** [*Faugère/Gianni/Lazard/Mora* JSC. 93, *Faugère/Mou* ISSAC'11].

Gröbner bases

$\mathcal{I}$ a **polynomial ideal**. Gröbner basis (w.r.t. a monomial ordering): $G \subset \mathcal{I}$ a finite set of polynomials such that $\mathrm{LM}(\mathcal{I}) = \langle \mathrm{LM}(G) \rangle$.

- **Buchberger** [*Buchberger* Ph.D. 65].
- $\mathbf{F_4}$ [*Faugère* J. of Pure and Appl. Alg. 99].
- $\mathbf{F_5}$ [*Faugère* ISSAC'02].
- **FGLM** [*Faugère/Gianni/Lazard/Mora* JSC. 93, *Faugère/Mou* ISSAC'11].

0-dimensional system solving

$$\textbf{Polynomial system} \xrightarrow{F_4/F_5} \text{grevlex GB} \xrightarrow{FGLM} \text{lex GB}.$$

Gröbner bases

$\mathcal{I}$ a **polynomial ideal**. Gröbner basis (w.r.t. a monomial ordering): $G \subset \mathcal{I}$ a finite set of polynomials such that $\mathsf{LM}(\mathcal{I}) = \langle \mathsf{LM}(G) \rangle$.

- **Buchberger** [*Buchberger* Ph.D. 65].
- **$\mathbf{F_4}$** [*Faugère* J. of Pure and Appl. Alg. 99].
- **$\mathbf{F_5}$** [*Faugère* ISSAC'02].
- **FGLM** [*Faugère/Gianni/Lazard/Mora* JSC. 93, *Faugère/Mou* ISSAC'11].

0-*dimensional system solving*

Polynomial system $\xrightarrow{F_4/F_5}$ grevlex GB $\xrightarrow{FGLM}$ lex GB.

XL/MXL

Most of the **complexity results** also valid for **XL**/**MXL**
Buchman/Bulygin/Cabarcas/Ding/Mohamed/Mohamed PQCrypto 2008, Africacrypt 2010,. . .
Ars/Faugère/Imai/Kawazoe/Sugita, Asiacrypt 2004
Albrecht/Cid/Faugère/Perret, eprint

0-dimensional system solving

Polynomial system $\xrightarrow{F_4/F_5}$ grevlex GB $\xrightarrow{FGLM}$ lex GB.

Lexicographical Gröbner basis of 0-dimensional systems

Equivalent system in **triangular** shape:

$$\begin{cases} f_1(x_1,\dots,x_n) &= 0 \\ & \vdots \\ f_\ell(x_1,\dots,x_n) &= 0 \\ f_{\ell+1}(x_2,\dots,x_n) &= 0 \\ & \vdots \\ f_{m-1}(x_{n-1},x_n) &= 0 \\ f_m(x_n) &= 0 \end{cases}$$

Gröbner bases (II)

0-dimensional system solving

Polynomial system $\xrightarrow{F_4/F_5}$ grevlex GB $\xrightarrow{FGLM}$ lex GB.

Lexicographical Gröbner basis of 0-dimensional systems

Equivalent system in **triangular** shape:

$$\left\{\begin{array}{rcl} f_1(x_1,\dots,x_n) & = & 0 \\ & \vdots & \\ f_\ell(x_1,\dots,x_n) & = & 0 \\ f_{\ell+1}(x_2,\dots,x_n) & = & 0 \\ & \vdots & \\ f_{m-1}(x_{n-1},x_n) & = & 0 \\ f_m(x_n) & = & 0 \end{array}\right. \Longrightarrow$$

Find the **roots** of **univariate** polynomials
$\rightarrow$ **easy** in finite fields.

$$\mathcal{I} = \langle f_1, \ldots, f_p \rangle \qquad \deg(f_i) = d_i \qquad \succ \text{ a monomial ordering}$$

Rows: all products tf_i where t is a monomial of degree at most $d - d_i$.
Columns: monomials of degree at most **d**.

$$\begin{array}{cc} & m_1 \succ \cdots \succ m_\ell \\ \begin{array}{c} t_1 f_1 \\ \vdots \\ t_k f_p \end{array} & \left(\begin{array}{c} \\ \\ \\ \end{array} \right) \end{array}$$

row echelon form of the **Macaulay matrix** with **d** sufficiently **high**

$\Longrightarrow$ **Gröbner basis**.

Macaulay matrix in degree d

$$\mathcal{I} = \langle f_1, \dots, f_p \rangle \qquad \deg(f_i) = d_i \qquad \succ \text{ a monomial ordering}$$

Rows: all products tf_i where t is a monomial of degree at most $d - d_i$.
Columns: monomials of degree at most **d**.

$$\begin{array}{cc} & m_1 \succ \cdots \succ m_\ell \\ \begin{array}{c} t_1 f_1 \\ \vdots \\ t_k f_p \end{array} & \left(\begin{array}{ccc} & & \\ & & \\ & & \end{array} \right) \end{array}$$

row echelon form of the **Macaulay matrix** with **d** sufficiently **high**

$$\Longrightarrow \textbf{Gröbner basis}.$$

Problems

- Degree falls.
- Rank defect $\rightsquigarrow$ useless computations.
  $\rightsquigarrow$**Hilbert series**: generating series of the **rank defects** of the Macaulay matrices.
- Which **d** ? $\rightsquigarrow$ **degree of regularity**.

Complexity of Gröbner bases computations

Two main indicators of the complexity

- **Degree of regularity** $\mathsf{d}_{\mathsf{reg}}$
  $\rightsquigarrow$ degree that has to be reached to compute the **grevlex GB**.
- **Degree of the ideal** $\mathcal{I} = \langle f_1, \ldots f_m \rangle$
  $\rightsquigarrow$ **Number of solutions** of the system (counted with multiplicities). Gives the **rank** of the Macaulay matrix.

Two main indicators of the complexity

- **Degree of regularity** $\mathsf{d}_{\mathsf{reg}}$
  $\rightsquigarrow$ degree that has to be reached to compute the **grevlex GB**.
- **Degree of the ideal** $\mathcal{I} = \langle f_1, \dots f_m \rangle$
  $\rightsquigarrow$ **Number of solutions** of the system (counted with multiplicities). Gives the **rank** of the Macaulay matrix.

	System $\longrightarrow$ grevlex GB	grevlex GB $\longrightarrow$ lex GB.
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d}_{\mathsf{reg}}}{\mathbf{d}_{\mathsf{reg}}}^{\omega}\right)$	$O\left(\mathbf{n} \cdot \#\mathbf{Sol}^{\omega}\right)$

Two main indicators of the complexity

- **Degree of regularity** $\mathsf{d}_{\mathsf{reg}}$
  $\rightsquigarrow$ degree that has to be reached to compute the **grevlex GB**.
- **Degree of the ideal** $\mathcal{I} = \langle f_1, \dots f_m \rangle$
  $\rightsquigarrow$ **Number of solutions** of the system (counted with multiplicities). Gives the **rank** of the Macaulay matrix.

	System $\longrightarrow$ grevlex GB $\longrightarrow$ lex GB.	
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d}_{\mathbf{reg}}}{\mathbf{d}_{\mathbf{reg}}}^{\omega}\right)$	$O\left(\mathbf{n} \cdot \#\mathbf{Sol}^{\omega}\right)$

Classical bounds (sharp for generic systems)

Let $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$ be a "generic" system.

- **Macaulay bound**: $\mathsf{d}_{\mathsf{reg}} \leq 1 + \sum_{1 \leq i \leq n} (d_i - 1)$.
- **Bézout bound**: $\deg(\langle f_1, \dots, f_n \rangle) \leq \prod_{1 \leq i \leq n} d_i$.

Complexity of Gröbner bases computations

Two main indicators of the complexity

- **Degree of regularity** $\mathsf{d}_{\mathsf{reg}}$
  $\rightsquigarrow$ degree that has to be reached to compute the **grevlex GB**.
- **Degree of the ideal** $\mathcal{I} = \langle f_1, \ldots f_m \rangle$
  $\rightsquigarrow$ **Number of solutions** of the system (counted with multiplicities). Gives the **rank** of the Macaulay matrix.

	System $\longrightarrow$ grevlex GB	grevlex GB $\longrightarrow$ lex GB.
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d}_{\mathsf{reg}}}{\mathbf{d}_{\mathsf{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot \#\mathbf{Sol}^{\omega}\right)$

Classical bounds (sharp for generic systems)

Let $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ be a "generic" system.

- **Macaulay bound**: $\mathsf{d}_{\mathsf{reg}} \leq 1 + \sum_{1\leq i\leq n} (d_i - 1)$.
- **Bézout bound**: $\deg(\langle f_1, \ldots, f_n \rangle) \leq \prod_{1\leq i\leq n} d_i$.

Are there sharper bounds for structured systems ?

Plan

1. Polynomial System Solving using Gröbner Bases
2. Bilinear Systems and Application to McEliece
3. Determinantal Systems and Applications to MinRank and HFE

Multi-homogeneous polynomial

$f \in \mathbb{K}[\underline{X}^{(1)}, \ldots, \underline{X}^{(\ell)}]$ is **multi-homogeneous** of multi-degree $(d_1, \ldots, d_\ell)$ if for all $\lambda_1, \ldots, \lambda_\ell$,

$$f(\lambda_1 \underline{X}^{(1)}, \ldots, \lambda_\ell \underline{X}^{(\ell)}) = \lambda_1^{d_1} \ldots \lambda_\ell^{d_\ell} f(\underline{X}^{(1)}, \ldots, \underline{X}^{(\ell)}).$$

Multi-homogeneous polynomial

$f \in \mathbb{K}[\underline{X}^{(1)}, \ldots, \underline{X}^{(\ell)}]$ is **multi-homogeneous** of multi-degree $(d_1, \ldots, d_\ell)$ if for all $\lambda_1, \ldots, \lambda_\ell$,

$$f(\lambda_1 \underline{X}^{(1)}, \ldots, \lambda_\ell \underline{X}^{(\ell)}) = \lambda_1^{d_1} \ldots \lambda_\ell^{d_\ell} f(\underline{X}^{(1)}, \ldots, \underline{X}^{(\ell)}).$$

Example:

$3x_1^2 y_1 + 4x_1 x_2 y_1 - 3x_2^2 y_1 - x_1^2 y_2 + 8x_1 x_2 y_2 - 5x_2^2 y_2 + 10x_1^2 y_3 - 2x_1 x_2 y_3 - 3x_2^2 y_3$ is a *bi-homogeneous polynomial* of bi-degree $(2, 1)$ in $\mathbb{F}_{11}[x_1, x_2, y_1, y_2, y_3]$.

Multi-homogeneous polynomial

$f \in \mathbb{K}[\underline{X}^{(1)}, \dots, \underline{X}^{(\ell)}]$ is **multi-homogeneous** of multi-degree $(d_1, \dots, d_\ell)$ if for all $\lambda_1, \dots, \lambda_\ell$,

$$f(\lambda_1 \underline{X}^{(1)}, \dots, \lambda_\ell \underline{X}^{(\ell)}) = \lambda_1^{d_1} \dots \lambda_\ell^{d_\ell} f(\underline{X}^{(1)}, \dots, \underline{X}^{(\ell)}).$$

Example:

$3x_1^2 y_1 + 4x_1 x_2 y_1 - 3x_2^2 y_1 - x_1^2 y_2 + 8x_1 x_2 y_2 - 5x_2^2 y_2 + 10x_1^2 y_3 - 2x_1 x_2 y_3 - 3x_2^2 y_3$
is a *bi-homogeneous polynomial* of bi-degree $(2, 1)$ in $\mathbb{F}_{11}[x_1, x_2, y_1, y_2, y_3]$.

Bilinear system: multi-homogeneous of multi-degree $(1, 1)$

$f_1, \dots, f_q \in \mathbb{K}[\underline{X}, \underline{Y}]$: **bilinear** forms.

$$f_k = \sum a_{i,j}^{(k)} x_i y_j.$$

Structure of bilinear systems

Euler relations

$f_1, \ldots, f_q \in \mathbb{K}[\underline{X}, \underline{Y}]$: **bilinear** forms.

$$f_k = \sum a_{i,j}^{(k)} x_i y_j.$$

Euler relations

$f_1, \ldots, f_q \in \mathbb{K}[\underline{X}, \underline{Y}]$: **bilinear** forms.

$$f_k = \sum a_{i,j}^{(k)} x_i y_j.$$

$$f_k = \sum_i \frac{\partial f_k}{\partial x_i} x_i = \sum_j \frac{\partial f_k}{\partial y_j} y_j.$$

Euler relations

$f_1, \ldots, f_q \in \mathbb{K}[\underline{X}, \underline{Y}]$: **bilinear** forms.

$f_k = \sum a_{i,j}^{(k)} x_i y_j$.

$$f_k = \sum_i \frac{\partial f_k}{\partial x_i} x_i = \sum_j \frac{\partial f_k}{\partial y_j} y_j.$$

$$\mathrm{jac}_x(F) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_q}{\partial x_1} & \cdots & \frac{\partial f_q}{\partial x_{n_x}} \end{pmatrix} \qquad \mathrm{jac}_y(F) = \begin{pmatrix} \frac{\partial f_1}{\partial y_1} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_q}{\partial y_1} & \cdots & \frac{\partial f_q}{\partial y_{n_y}} \end{pmatrix}.$$

$$\Longrightarrow \begin{pmatrix} f_1 \\ \vdots \\ f_q \end{pmatrix} = \mathrm{jac}_x(F) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n_x} \end{pmatrix} = \mathrm{jac}_y(F) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_{n_y} \end{pmatrix}.$$

$$\begin{pmatrix} f_1 \\ \vdots \\ f_q \end{pmatrix} = \mathrm{jac}_x(F) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n_x} \end{pmatrix}.$$

If $(x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y})$ is a *non-trivial solution* of F, then $\mathrm{jac}_x(F)$ is **rank defective**.

$\rightsquigarrow$ $(y_1, \ldots, y_{n_y})$ is a zero of the **maximal minors** of $\mathrm{jac}_x(F)$.

Something special happens with minors...

$$\begin{pmatrix} f_1 \\ \vdots \\ f_q \end{pmatrix} = \mathrm{jac}_x(F) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n_x} \end{pmatrix}.$$

If $(x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y})$ is a *non-trivial solution* of F, then $\mathrm{jac}_x(F)$ is **rank defective**.

$\rightsquigarrow$ $(y_1, \ldots, y_{n_y})$ is a zero of the **maximal minors** of $\mathrm{jac}_x(F)$.

Bernstein/Sturmfels/Zelevinski, Adv. in Math. 1993

M a $p \times q$ **matrix** whose entries are **variables**. For any monomial ordering, the maximal minors of M are a Gröbner basis of the associated ideal.

Something special happens with minors...

$$\begin{pmatrix} f_1 \\ \vdots \\ f_q \end{pmatrix} = \mathrm{jac}_x(F) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n_x} \end{pmatrix}.$$

If $(x_1, \dots, x_{n_x}, y_1, \dots, y_{n_y})$ is a *non-trivial solution* of F, then $\mathrm{jac}_x(F)$ is **rank defective**.

$\rightsquigarrow$ $(y_1, \dots, y_{n_y})$ is a zero of the **maximal minors** of $\mathrm{jac}_x(F)$.

Bernstein/Sturmfels/Zelevinski, Adv. in Math. 1993

M a $p \times q$ **matrix** whose entries are **variables**. For any monomial ordering, the maximal minors of M are a Gröbner basis of the associated ideal.

Faugère/Safey El Din/S., J. of Symb. Comp. 2011

M a k-variate $q \times p$ **linear matrix** (with $q > p$). Generically, a grevlex GB of $\langle \mathrm{Minors}(M) \rangle$: **linear combination** of the generators.

$$\rightsquigarrow \mathrm{d}_{\mathrm{reg}}\left(\mathrm{MaxMinors}(\mathrm{jac}_x(F))\right) = n_x.$$

Complexity

Affine bilinear polynomial

$f \in \mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$ is said to be **affine bilinear** if there exists a **bilinear polynomial** $\tilde{f}$ in $\mathbb{K}[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$ such that

$$f(x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}) = \tilde{f}(1, x_1, \ldots, x_{n_x}, 1, y_1, \ldots, y_{n_y}).$$

Faugère/Safey El Din/S., J. of Symb. Comp. 2011

Degree of regularity

Let $f_1, \ldots, f_{n_x+n_y}$ be an **affine bilinear system** in $\mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$. Then the **highest degree** reached during the computation of a **Gröbner basis** for the *grevlex* ordering is upper bounded by

$$\min(\mathbf{n_x}, \mathbf{n_y}) + \mathbf{1} \ll n_x + n_y + 1.$$

Complexity

Affine bilinear polynomial

$f \in \mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$ is said to be **affine bilinear** if there exists a **bilinear polynomial** $\tilde{f}$ in $\mathbb{K}[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$ such that

$$f(x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}) = \tilde{f}(1, x_1, \ldots, x_{n_x}, 1, y_1, \ldots, y_{n_y}).$$

Faugère/Safey El Din/S., J. of Symb. Comp. 2011

Degree of regularity

Let $f_1, \ldots, f_{n_x+n_y}$ be an **affine bilinear system** in $\mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$. Then the **highest degree** reached during the computation of a **Gröbner basis** for the *grevlex* ordering is upper bounded by

$$\min(\mathbf{n_x}, \mathbf{n_y}) + \mathbf{1} \ll n_x + n_y + 1.$$

Consequences

- The complexity of computing a **grevlex GB** is **polynomial** in the number of solutions !!
- **Bilinear** systems with unbalanced sizes of blocks of variables are **easy to solve** !!

Based on **alternant codes**:

- secret key: a **parity-check** matrix of the form

$$H = \begin{pmatrix} y_0 & y_1 & \dots & y_{n-1} \\ y_0 x_0 & y_1 x_1 & \dots & y_{n-1} x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_0 x_0^{t-1} & y_1 x_1^{t-1} & \dots & y_n x_n^{t-1} \end{pmatrix},$$

  where $x_i, y_j \in \mathbb{F}_{2^m}$, with $x_0, \dots, x_n$ pairwise distinct and $y_j \neq 0$.
- public key: a **generator matrix** G of the same code.

Based on **alternant codes**:

- secret key: a **parity-check** matrix of the form

$$H = \begin{pmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_0 x_0 & y_1 x_1 & \cdots & y_{n-1} x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_0 x_0^{t-1} & y_1 x_1^{t-1} & \cdots & y_n x_n^{t-1} \end{pmatrix},$$

  where $x_i, y_j \in \mathbb{F}_{2^m}$, with $x_0, \ldots, x_n$ pairwise distinct and $y_j \neq 0$.
- public key: a **generator matrix** G of the same code.

Problem

Given G, find H such that $H \cdot G^t = 0$!

Modeling of McEliece cryptosystem

Based on **alternant codes**:

- secret key: a **parity-check** matrix of the form

$$H = \begin{pmatrix} y_0 & y_1 & \dots & y_{n-1} \\ y_0 x_0 & y_1 x_1 & \dots & y_{n-1} x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_0 x_0^{t-1} & y_1 x_1^{t-1} & \dots & y_n x_n^{t-1} \end{pmatrix},$$

  where $x_i, y_j \in \mathbb{F}_{2^m}$, with $x_0, \dots, x_n$ pairwise distinct and $y_j \neq 0$.
- public key: a **generator matrix** G of the same code.

Problem

Given G, find H such that $H \cdot G^t = \mathbf{0}$!

$$\rightsquigarrow \forall i,j, \quad g_{i,0} y_0 x_0^j + \dots + g_{i,n-1} y_{n-1} x_{n-1}^j = 0.$$

$\Rightarrow$ **Bi-homogeneous structure** !!

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

$\Rightarrow$ add **redundancy** to the polynomial system
$\rightsquigarrow$ linear equations $\rightsquigarrow$ less variables.

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

$\Rightarrow$ add **redundancy** to the polynomial system
$\leadsto$ linear equations $\leadsto$ less variables.
Moreover, the system is still over-determined and one can extract a subsystem containing only **powers of two**:

$$\leadsto \forall i, j \text{ **a power of two** !!}, \quad g_{i,0}\, y_0\, x_0^j + \cdots + g_{i,n-1}\, y_{n-1}\, x_{n-1}^j = 0.$$

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

$\Rightarrow$ add **redundancy** to the polynomial system
$\rightsquigarrow$ linear equations $\rightsquigarrow$ less variables.
Moreover, the system is still over-determined and one can extract a subsystem containing only **powers of two**:

$$\rightsquigarrow \forall i,j \textbf{ a power of two !!}, \quad g_{i,0}y_0x_0^j + \cdots + g_{i,n-1}y_{n-1}x_{n-1}^j = 0.$$

Decomposing the subsystem over the field $\mathbb{F}_2$

$\Rightarrow$ **Bilinear system with $n_x \ll n_y$!!!**

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczy/Barreto SAC'09.

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

$\Rightarrow$ add **redundancy** to the polynomial system
$\rightsquigarrow$ linear equations $\rightsquigarrow$ less variables.
Moreover, the system is still over-determined and one can extract a subsystem containing only **powers of two**:

$$\rightsquigarrow \forall i, j \textbf{ a power of two !!}, \quad g_{i,0} y_0 x_0^j + \cdots + g_{i,n-1} y_{n-1} x_{n-1}^j = 0.$$

Decomposing the subsystem over the field $\mathbb{F}_2$

$$\Rightarrow \textbf{Bilinear system with } n_x \ll n_y \textbf{ !!!}$$

Theoretical and **Practical attacks** on the quasi-cyclic and dyadic variants of McEliece !!

Plan

$r \in \mathbb{N}$. $M_0, \ldots, M_k$: $k+1$ matrices of size $m \times m$.

MinRank

find $\lambda_1, \ldots, \lambda_k$ such that

$$\mathbf{Rank}\left(M_0 - \sum_{i=1}^{k} \lambda_i M_i\right) \le r.$$

- **Multivariate** generalization of the **Eigenvalue** problem.
- Applications in **cryptology**, **coding theory**, …
  Kipnis/Shamir Crypto'99, *Courtois* Asiacrypt'01
  Faugère/Levy-dit-Vehel/Perret Crypto'08,...
- Fundamental **NP-hard** problem of **linear algebra**.

Buss, Frandsen, Shallit.
The computational complexity of some problems of linear algebra.

$$\mathbf{M} = M_0 - \sum_{i=1}^{k} \lambda_i M_i.$$

$$\mathbf{M} = M_0 - \sum_{i=1}^{k} \lambda_i M_i.$$

The minors modeling

$$\textbf{Rank}(\mathbf{M}) \leq r$$
$$\Updownarrow$$
all minors of size $(r+1)$ of $\mathbf{M}$ vanish.

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

Few variables, lots of equations, high degree !!

$$\mathbf{M} = M_0 - \sum_{i=1}^{k} \lambda_i M_i.$$

The minors modeling

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

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

Few variables, lots of equations, high degree !!

The Kipnis-Shamir modeling

$\mathbf{Rank}(\mathbf{M}) \leq r \Leftrightarrow \exists x^{(1)}, \ldots, x^{(m-r)} \in \mathbf{Ker}(\mathbf{M})$.

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

- $m(m-r)$ bilinear equations.
- $k + r(m-r)$ variables.

$$\mathbf{M} = M_0 - \sum_{i=1}^{k} \lambda_i M_i.$$

The minors modeling

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

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

Few variables, lots of equations, high degree !!

The Kipnis-Shamir modeling

$\mathbf{Rank}(\mathbf{M}) \leq r \Leftrightarrow \exists x^{(1)}, \ldots, x^{(m-r)} \in \mathbf{Ker}(\mathbf{M})$.

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

- $m(m-r)$ bilinear equations.
- $k + r(m-r)$ variables.

- **Complexity** of solving MinRank using Gröbner bases techniques ?
- **Comparison** of the two modelings ?
- **Number** of solutions ?

Main results

	System $\longrightarrow$ grevlex GB $\longrightarrow$ lex GB.	
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d_{reg}}}{\mathbf{d_{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^{\omega}\right)$

	System $\longrightarrow$ grevlex GB $\longrightarrow$ lex GB.	
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d}_{\mathrm{reg}}}{\mathbf{d}_{\mathrm{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^{\omega}\right)$

m: size of the matrices, **k**: number of matrices, **r**: target rank. $\mathbf{k}=(\mathbf{m}-\mathbf{r})^2$.

Modeling:	Minors	Kipnis-Shamir
Degree of regularity when $k=(m-r)^2$		Macaulay bound: $\leq m(m-r)+1$
# Sol	MH. Bézout: $\leq \binom{m}{r}^{m-r}$	
Complexity		

Main results

	System $\longrightarrow$ grevlex GB $\longrightarrow$ lex GB.	
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d_{reg}}}{\mathbf{d_{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^{\omega}\right)$

m: size of the matrices, **k**: number of matrices, **r**: target rank. $\mathbf{k}=(\mathbf{m}-\mathbf{r})^2$.

Modeling:	Minors	Kipnis-Shamir
Degree of regularity when $k=(m-r)^2$		$\leq (m-r)^2+1$
# Sol	MH. Bézout: $\leq \binom{m}{r}^{m-r}$	
Complexity		

	System $\longrightarrow$ grevlex GB $\longrightarrow$ lex GB.	
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d_{reg}}}{\mathbf{d_{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^{\omega}\right)$

$\mathbf{m}$: size of the matrices, $\mathbf{k}$: number of matrices, $\mathbf{r}$: target rank. $\mathbf{k} = (\mathbf{m}-\mathbf{r})^2$.

Modeling:	Minors	Kipnis-Shamir
Degree of regularity when $k=(m-r)^2$	$r(m-r)+1$	$\leq (m-r)^2+1$
# Sol	MH. Bézout: $\leq \binom{m}{r}^{m-r}$	
Complexity		

Main results

	System $\longrightarrow$ grevlex GB	$\longrightarrow$ lex GB.
Algorithms	grevlex GB	Change of Ordering
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d}_{\mathrm{reg}}}{\mathbf{d}_{\mathrm{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^{\omega}\right)$

$\mathbf{m}$: size of the matrices, $\mathbf{k}$: number of matrices, $\mathbf{r}$: target rank. $\mathbf{k}=(\mathbf{m}-\mathbf{r})^2$.

Modeling:	Minors	Kipnis-Shamir
Degree of regularity when $k=(m-r)^2$	$r(m-r)+1$	$\leq (m-r)^2+1$
# Sol	$\prod_{i=0}^{m-r-1}\frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$	
Complexity		

Main results

	System $\longrightarrow$ grevlex GB $\longrightarrow$ lex GB.	
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d_{reg}}}{\mathbf{d_{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^{\omega}\right)$

m: size of the matrices, **k**: number of matrices, **r**: target rank. $\mathbf{k} = (\mathbf{m}-\mathbf{r})^2$.

Modeling:	Minors	Kipnis-Shamir
Degree of regularity when $k = (m-r)^2$	$r(m-r)+1$	$\leq (m-r)^2+1$
# Sol	$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$	
Complexity	$O(m^{\omega k})$	$O(m^{\omega(k+1)})$

Main results

	System $\longrightarrow$ grevlex GB $\longrightarrow$ lex GB.	
Algorithms	*grevlex GB*	*Change of Ordering*
Complexity	$O\left(\binom{\mathbf{n}+\mathbf{d_{reg}}}{\mathbf{d_{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot\#\mathbf{Sol}^{\omega}\right)$

m: size of the matrices, **k**: number of matrices, **r**: target rank. $\mathbf{k}=(\mathbf{m}-\mathbf{r})^2$.

Modeling:	Minors	Kipnis-Shamir
Degree of regularity when $k=(m-r)^2$	$r(m-r)+1$	$\leq (m-r)^2+1$
# Sol	$\prod_{i=0}^{m-r-1}\frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$	
Complexity	$O(m^{\omega k})$	$O(m^{\omega(k+1)})$

Both modelings $\rightarrow$ polynomial complexity when $\mathbf{k}=(\mathbf{m}-\mathbf{r})^2$ is fixed.

New Crypto challenge broken: 10 generic matrices of size 11×11
target rank 8, $\mathbb{K}=\mathrm{GF}(65521)$.
Courtois, Asiacrypt 2001.

Minors modeling:

$$\boxed{\begin{array}{c}\textbf{Rank}(\mathbf{M}) \leq r \\ \Updownarrow \\ \text{all minors of size } (r+1) \text{ of } \mathbf{M} \text{ vanish.}\end{array}}$$

$\rightsquigarrow$ **Determinantal ideal**

Minors modeling:

$$\boxed{\begin{array}{c}\mathbf{Rank}(\mathbf{M}) \leq r \\ \Updownarrow \\ \text{all minors of size } (r+1) \text{ of } \mathbf{M} \text{ vanish.}\end{array}}$$

$\rightsquigarrow$ **Determinantal ideal**

Bilinear systems $\leftrightarrow$ determinantal systems

$f_1, \ldots, f_q \in \mathbb{K}[\underline{X}, \underline{Y}]$: bilinear forms.

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_q}{\partial x_0} & \cdots & \frac{\partial f_q}{\partial x_{n_x}} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_q \end{pmatrix}$$

$$f_1 = \ldots = f_q = 0 \iff \mathrm{MaxMinors}\left(\mathrm{Jac}_X(f_1, \ldots, f_q)\right) = 0.$$

Determinantal ideals

What is known

- **Determinantal** ideals: *Bernstein/Zelevinsky* J. of Alg. Comb. 93, *Bruns/Conca* 98, *Sturmfels/Zelevinsky* Adv. Math. 98, *Conca/Herzog* AMS'94, *Lascoux* 78, *Abhyankar* 88...
- **Geometry** of determinantal varieties: *Room* 39, *Fulton* Duke Math. J. 91, *Giusti/Merle* Int. Conf. on Alg. Geo. 82...
- **Polar varieties**: *Bank/Giusti/Heintz/Safey/Schost* AAECC'10,*Bank/Giusti/Heintz/Pardo* J. of Compl. 05, *Safey/Schost* ISSAC'03, *Teissier* Pure and Appl. Math. 91...

Properties of Determinantal Ideals

$$\mathcal{D} = \text{Minors}_{r+1}\begin{pmatrix} v_{1,1} & \cdots & v_{1,m} \\ \vdots & \ddots & \vdots \\ v_{m,1} & \cdots & v_{m,m} \end{pmatrix}$$

Thom, Porteous, Giambelli, Harris-Tu, ...

The **degree** of $\mathcal{D}$ is

$$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}.$$

Conca/Herzog, Abhyankar

The **Hilbert series** of $\mathcal{D}$ is

$$\text{HS}_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{(2m-r)r}}.$$

$$A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell}\binom{m-j}{\ell} t^{\ell}.$$

$$\textcolor{red}{\mathcal{D}} = \mathrm{Minors}_{r+1}\begin{pmatrix} v_{1,1} & \cdots & v_{1,m} \\ \vdots & \ddots & \vdots \\ v_{m,1} & \cdots & v_{m,m} \end{pmatrix}$$

Thom, Porteous, Giambelli, Harris-Tu, ...
The **degree** of $\mathcal{D}$ is

$$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}.$$

Conca/Herzog, Abhyankar
The **Hilbert series** of $\mathcal{D}$ is

$$\mathrm{HS}_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{(2m-r)r}}.$$

$$\textcolor{red}{\mathcal{I}} = \mathrm{Minors}_{r+1}\begin{pmatrix} f_{1,1} & \cdots & f_{1,m} \\ \vdots & \ddots & \vdots \\ f_{m,1} & \cdots & f_{m,m} \end{pmatrix}$$

$$A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell}\binom{m-j}{\ell} t^{\ell}.$$

$$\mathcal{D} = \mathrm{Minors}_{r+1}\begin{pmatrix} v_{1,1} & \cdots & v_{1,m} \\ \vdots & \ddots & \vdots \\ v_{m,1} & \cdots & v_{m,m} \end{pmatrix}$$

Thom, Porteous, Giambelli, Harris-Tu, ...
The **degree** of $\mathcal{D}$ is

$$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}.$$

Conca/Herzog, Abhyankar
The **Hilbert series** of $\mathcal{D}$ is

$$\mathrm{HS}_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{(2m-r)r}}.$$

$$\mathcal{I} = \mathrm{Minors}_{r+1}\begin{pmatrix} f_{1,1} & \cdots & f_{1,m} \\ \vdots & \ddots & \vdots \\ f_{m,1} & \cdots & f_{m,m} \end{pmatrix}$$

$$A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell}\binom{m-j}{\ell} t^{\ell}.$$

transfer of properties of $\mathcal{D}$ by adding $\langle v_{i,j} - f_{i,j}\rangle$

$$\mathcal{D} = \mathrm{Minors}_{r+1}\begin{pmatrix} v_{1,1} & \cdots & v_{1,m} \\ \vdots & \ddots & \vdots \\ v_{m,1} & \cdots & v_{m,m} \end{pmatrix}$$

Thom, Porteous, Giambelli, Harris-Tu, ...
The **degree** of $\mathcal{D}$ is

$$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}.$$

Conca/Herzog, Abhyankar
The **Hilbert series** of $\mathcal{D}$ is

$$\mathrm{HS}_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{(2m-r)r}}.$$

$$\mathcal{I} = \mathrm{Minors}_{r+1}\begin{pmatrix} f_{1,1} & \cdots & f_{1,m} \\ \vdots & \ddots & \vdots \\ f_{m,1} & \cdots & f_{m,m} \end{pmatrix}$$

ISSAC'2010
The **degree** of $\mathcal{I}$ is

$$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}.$$

ISSAC'2010
The **Hilbert series** of $\mathcal{I}$ is

$$\mathrm{HS}_{\mathcal{I}}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{k-(m-r)^2}}.$$

$$A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell}\binom{m-j}{\ell} t^{\ell}.$$

transfer of properties of $\mathcal{D}$ by adding $\langle v_{i,j} - f_{i,j} \rangle$

Degree of regularity for a 0-dim ideal $=$ 1$+$ degree of the **Hilbert series**.

Corollary

The **degree of regularity** of $\mathcal{I}$ is generically equal to

$$\mathbf{d}_{\mathsf{reg}} = r(m-r)+1.$$

Degree of regularity for a 0-dim ideal = 1+ degree of the **Hilbert series**.

Corollary

The **degree of regularity** of $\mathcal{I}$ is generically equal to

$$\mathbf{d}_{\mathbf{reg}} = r(m-r)+1.$$

Number of matrices and rank defect fixed. 0-dimensional case.

Corollary: asymptotic complexity

When $k=(m-r)^2$ is fixed, then the **complexity** of the **Gröbner basis** computation of the **minors** modeling is

$$O\left(m^{\omega k}\right).$$

Corollary: generic number of solutions

The **number of solutions** of a **generic MinRank** problem with $k = (m - r)^2$ is

$$\begin{aligned}\#Sol \quad &= \quad \prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!} \\ &\underset{m\to\infty}{\sim} \quad m^k \prod_{i=0}^{m-r-1} \frac{i!}{(m-r+i)!}.\end{aligned}$$

Complexity of the Change of Ordering

Corollary: generic number of solutions

The **number of solutions** of a **generic MinRank** problem with $k = (m-r)^2$ is

$$\begin{aligned} \#Sol &= \prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!} \\ &\underset{m\to\infty}{\sim} m^k \prod_{i=0}^{m-r-1} \frac{i!}{(m-r+i)!}. \end{aligned}$$

Complexity of the Change of Ordering (ISSAC 2010)

The **complexity of FGLM** is upper bounded by $O(\#Sol^{\omega})$.
If $k = (m-r)^2$, then

$$O(\#Sol^{\omega}) = O\left(m^{\omega k}\right).$$

Courtois. Asiacrypt'01.

Efficient zero-knowledge authentication based on a linear algebra problem MinRank.

$\mathbb{K} = \mathbf{GF(65521)}$ $\mathbf{(m, k, r)}$: k matrices of size $m \times m$. Target rank: r.

Challenge	**A**	**B**			**C**
	$(6,9,3)$	$(7,9,4)$	$(8,9,5)$	$(9,9,6)$	$(11,9,8)$
degree	**980**	**4116**	**14112**	**41580**	259545
	Minors modeling				
d_{reg}	10	13	16	19	
F_5 time	**1.1s**	**28.4s**	**544s**	**9048s**	-
F_5 mem	**488 MB**	**587 MB**	**1213 MB**	**5048 MB**	-
$\log_2$(Nb op.)	**21.5**	**25.9**	**29.2**	**32.7**	
FGLM time	**0.5s**	**28.5s**	**1033s**	**22171s**	-
	Kipnis-Shamir modeling				
d_{reg}	5	6	7		
F_5 time	**30s**	**3795s**	**328233s**	∞	
F_5 mem	**407 MB**	**3113 MB**	**58587 MB**		
$\log_2$(Nb op.)	**30.5**	**37.1**	**43.4**		
FGLM time	**35s**	**2580s**	∞		

Courtois. Asiacrypt'01.
Efficient zero-knowledge authentication based on a linear algebra problem MinRank.

$\mathbb{K} = \mathbf{GF(65521)}$ $\quad$ $(\mathbf{m}, \mathbf{k}, \mathbf{r})$: k matrices of size $m \times m$. Target rank: r.

Challenge	**A**	**B**			**C**
	$(6,9,3)$	$(7,9,4)$	$(8,9,5)$	$(9,9,6)$	$(11,9,8)$
degree	**980**	**4116**	**14112**	**41580**	259545
	Minors modeling				
d_{reg}	10	13	16	19	
F_5 time	**1.1s**	**28.4s**	**544s**	**9048s**	-
F_5 mem	**488 MB**	**587 MB**	**1213 MB**	**5048 MB**	-
$\log_2$(Nb op.)	**21.5**	**25.9**	**29.2**	**32.7**	
FGLM time	**0.5s**	**28.5s**	**1033s**	**22171s**	-
	Kipnis-Shamir modeling				
d_{reg}	5	6	7		
F_5 time	**30s**	**3795s**	**328233s**	∞	
F_5 mem	**407 MB**	**3113 MB**	**58587 MB**		
$\log_2$(Nb op.)	**30.5**	**37.1**	**43.4**		
FGLM time	**35s**	**2580s**	∞		

Computational bottleneck: computing the minors.
Computing effort needed for solving **Challenge C**:
238 days on 64 quadricore processors.

Patarin, Eurocrypt'96
Billet/Patarin/Seurin, ICSCC'08
Ding/Schmitt/Werner, Information Security, 2008

$$P(x) = \sum_{0 \leq i,j \leq r} p_{i,j} x^{q^i + q^j} \in \mathbb{F}_{q^n}, \text{ with } r \ll n$$

$\rightsquigarrow$ **low-rank** quadratic form $(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$

Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt'96
Billet/Patarin/Seurin, ICSCC'08
Ding/Schmitt/Werner, Information Security, 2008

$$P(x) = \sum_{0 \leq i,j \leq r} p_{i,j} x^{q^i + q^j} \in \mathbb{F}_{q^n}, \text{ with } r \ll n$$

$\rightsquigarrow$ **low-rank** quadratic form $(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$
masked by linear transforms !!

Patarin, Eurocrypt'96
Billet/Patarin/Seurin, ICSCC'08
Ding/Schmitt/Werner, Information Security, 2008

$$P(x) = \sum_{0 \le i,j \le r} p_{i,j} x^{q^i + q^j} \in \mathbb{F}_{q^n}, \text{ with } r \ll n$$

$\rightsquigarrow$ **low-rank** quadratic form $(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$
masked by linear transforms !!

$\Rightarrow$ the **secret polynomial** can be recovered by solving a **MinRank problem**.

Bettale/Faugère/Perret, PKC 2011

The **complexity** of solving this MinRank problem is upper bounded by

$$O\left(n^{(r+1)\omega}\right).$$

- $\rightsquigarrow$ algebraic attack with **polynomial complexity** in n !!
- $\rightsquigarrow$ attacks on **odd-characteristic** variants;
- $\rightsquigarrow$ generalizations to **multi-HFE**.

Conclusion and Perspectives

Structures have an impact on the complexity of the solving process in algebraic cryptanalysis !

Design, key **size reduction**,... $\overset{\text{Structure}}{\longleftrightarrow}$ potential **algebraic attacks**.

Structures have an impact on the complexity of the solving process in algebraic cryptanalysis !

Design, key **size reduction**,... $\overset{\text{Structure}}{\longleftrightarrow}$ potential **algebraic attacks**.

Other possible applications in Crypto of structured systems

- **Rank metric codes** (*Gabidulin/Ourivski/Honary/Ammar IEEE IT, 2003*).
- classical **McEliece** PKC (*McEliece 1978*).

Structures have an impact on the complexity of the solving process in algebraic cryptanalysis !

Design, key **size reduction**,... $\overset{\textbf{Structure}}{\longleftrightarrow}$ potential **algebraic attacks**.

Other possible applications in Crypto of structured systems

- **Rank metric codes** (*Gabidulin/Ourivski/Honary/Ammar IEEE IT, 2003*).
- classical **McEliece** PKC (*McEliece 1978*).

Algorithmic problems

- Dedicated F_5 algorithm for multi-homogeneous systems.
  $\rightsquigarrow$ (*Faugère, Safey, S., J. of Symb. Comp. 2011*)
- Dedicated algorithm for **determinantal systems** ?