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
Algebraic Cryptanalysis

Crypto primitive

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

Structure?
Algebraic Cryptanalysis

Crypto primitive

modeling

\[
\begin{align*}
2x^2 + 2y^2 + 2z^2 + 2t^2 + 2u^2 + v^2 - v &= 0 \\
2xy + 2yz + 2zt + 2tu + 2uv - u &= 0 \\
2xz + 2yt + 2zu + u^2 + 2tu - t &= 0 \\
2xt + 2yu + 2zu + 2uv - z &= 0 \\
x^2 + 2xy + 2yu + 2uz - y &= 0 \\
2x + 2y + 2z + 2t + 2u + v - 1 &= 0
\end{align*}
\]
Algebraic Cryptanalysis

Crypto primitive

modeling

System solving

\[
\begin{align*}
f_1(X_1) &= 0 \\
f_2(X_1, X_2) &= 0 \\
&\vdots \\
f_{2g_1}(X_1, X_2) &= 0 \\
f_{2g_1+1}(X_1, X_2, X_3) &= 0 \\
&\vdots \\
f_{2g_1+g_2}(X_1, \ldots, X_n) &= 0 \\
f_{2g_1+g_2+1}(X_1, \ldots, X_n) &= 0
\end{align*}
\]

\[
\begin{align*}
2x^2 + 2y^2 + 2z^2 + 2t^2 + 2u^2 + v^2 - v &= 0 \\
2xy + 2yz + 2zt + 2tu + 2uv - u &= 0 \\
2xs + 2yt + 2zu + u^2 + 2tv - t &= 0 \\
2xt + 2yu + 2zu + 2xv - z &= 0 \\
2l + 2xu + 2yu + 2xv - y &= 0 \\
2x + 2y + 2z + 2t + 2u + v - l &= 0
\end{align*}
\]
Issues

- Which \textit{algebraic modeling}?
- Tradeoff between the \textit{degree} of the equations/number of \textit{variables}?
- Solving tools: \textit{Gröbner bases}? \textit{SAT-solvers}? ...
- \textit{Structure}?
Motivations: Algebraic Structures in Cryptology

Where does the structure come from?

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

Asymmetric encryption/signature: ⇝ trapdoor (e.g. HFE, Multi-HFE, McEliece).

⇝ Reducing the key sizes is a common issue → potential weaknesses due to the structure.

Symmetries, invariants: ⇝ invariance of the solutions under some transformations (e.g. MinRank).

Impact on the solving process? Complexity? Dedicated algorithms?
Where does the **structure** come from?

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

- **Asymmetric encryption/signature:**
  - Trapdoor (e.g. HFE, Multi-HFE, McEliece).
  - Reducing the **key sizes** is a common issue → potential **weaknesses** due to the structure.
Where does the **structure** come from?

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

- **Asymmetric encryption/signature:**
  
  - trapdoor (e.g. HFE, Multi-HFE, McEliece).
  - Reducing the **key sizes** is a common issue
    → potential **weaknesses** due to the structure.

- **Symmetries, invariants:**
  
  - **invariance of the solutions** under some transformations (e.g. MinRank).

- ...
Where does the structure come from?

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

- **Asymmetric encryption/signature:**
  - **trapdoor** (e.g. HFE, Multi-HFE, McEliece).
  - Reducing the **key sizes** is a common issue
    - → potential **weaknesses** due to the structure.

- **Symmetries, invariants:**
  - **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 → Security**
  - Sometimes bi(or multi)-linear
    - (e.g. AES S-boxes: $x \cdot y - 1 = 0$ for $x \neq 0$).

- **Asymmetric encryption/signature:**
  - **trapdoor** (e.g. HFE, Multi-HFE, McEliece).
  - Reducing the **key sizes** is a common issue
    - → potential **weaknesses** due to the structure.

- **Symmetries, invariants:**
  - **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.
- ...

Determinantal systems

Cryptosystems based on rank metric codes.

Hidden Field Equations and variants.

Systems invariant by symmetries

Discrete log on elliptic and hyperelliptic curves.
## 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.
- ...

4/28  PJ Spaenlehauer
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.
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 (I)

Gröbner bases

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

- **Buchberger** [Buchberger Ph.D. 65].
- **F4** [Faugère J. of Pure and Appl. Alg. 99].
- **F5** [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): \( G \subseteq \mathcal{I} \) a finite set of polynomials such that \( \text{LM}(\mathcal{I}) = \langle \text{LM}(G) \rangle \).

- **Buchberger** [Buchberger Ph.D. 65].
- **F₄** [Faugère J. of Pure and Appl. Alg. 99].
- **F₅** [Faugère ISSAC’02].
- **FGLM** [Faugère/Gianni/Lazard/Mora JSC. 93, Faugère/Mou ISSAC’11].

**0-dimensional system solving**

Polynomial system \( \xrightarrow{F₄/F₅} \text{grevlex GB} \xrightarrow{\text{FGLM}} \text{lex GB}. \)
Gröbner bases (I)

Gröbner bases

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

- **Buchberger** \([Buchberger Ph.D. 65]\).
- **F₄** \([Faugère J. of Pure and Appl. Alg. 99]\).
- **F₅** \([Faugère ISSAC’02]\).
- **FGLM** \([Faugère/Gianni/Lazard/Mora JSC. 93, Faugère/Mou ISSAC’11]\).

0-dimensional system solving

Polynomial system \( \frac{F₄}{F₅} \rightarrow \text{grevlex GB} \rightarrow \frac{\text{FGLM}}{\text{lex GB}} \).

XL/MXL

Most of the complexity results also valid for **XL/MXL**

\textbf{Buchman/Bulygin/Cabarcas/Ding/Mohamed/Mohamed PQCrypto 2008, Africacrypt 2010, ...}

\textbf{Ars/Faugère/Imai/Kawazoe/Sugita, Asiacrypt 2004}

\textbf{Albrecht/Cid/Faugère/Perret, eprint}
Gröbner bases (II)

0-dimensional system solving

Polynomial system $\frac{F_4}{F_5} \rightarrow \text{grevlex GB} \rightarrow \text{lex GB}$.

Lexicographical Gröbner basis of 0-dimensional systems

Equivalent system in triangular shape:

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

$\Rightarrow$ Find the roots of univariate polynomials $\rightarrow$ easy in infinite fields.
0-dimensional system solving

**Polynomial system**

\[ \frac{F_4}{F_5} \rightarrow \text{grevlex GB} \rightarrow \text{lex GB}. \]

**Lexicographical Gröbner basis of 0-dimensional systems**

Equivalent system in **triangular** shape:

\[
\begin{align*}
    f_1(x_1, \ldots, x_n) &= 0 \\
    f_2(x_1, \ldots, x_n) &= 0 \\
    & \quad \vdots \\
    f_\ell(x_1, \ldots, x_n) &= 0 \\
    f_{\ell+1}(x_2, \ldots, x_n) &= 0 \\
    & \quad \vdots \\
    f_{m-1}(x_{n-1}, x_n) &= 0 \\
    f_m(x_n) &= 0
\end{align*}
\]

Find the roots of **univariate** polynomials \( \rightarrow \) easy in finite fields.
Macaulay matrix in degree $d$

$I = \langle f_1, \ldots, f_p \rangle \quad \text{deg}(f_i) = d_i \quad \succ$ 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 $d$.

\[
\begin{pmatrix}
  t_1 f_1 \\
  \vdots \\
  t_k f_p
\end{pmatrix}
\]

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

$\implies$ **Gröbner basis.**
Macaulay matrix in degree $d$

$\mathcal{I} = \langle f_1, \ldots, f_p \rangle$ \quad $\deg(f_i) = d_i$ \quad $\succ$ \quad 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 $d$.

\[
\begin{pmatrix}
    t_1 f_1 \\
    \vdots \\
    t_k f_p
\end{pmatrix} \quad m_1 \succ \cdots \succ m_\ell
\]

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

$\implies$ **Gröbner basis.**

---

**Problems**

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

- **Degree of regularity** $d_{\text{reg}}$
  - Degree that has to be reached to compute the *grevlex* GB.

- **Degree of the ideal** $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$
  - 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** \( d_{\text{reg}} \)
  - \( d_{\text{reg}} \) is the degree that has to be reached to compute the **grevlex GB**.

- **Degree of the ideal** \( \mathcal{I} = \langle f_1, \ldots, f_m \rangle \)
  - \( d_{\text{reg}} \) is the **number of solutions** of the system (counted with multiplicities). Gives the **rank** of the Macaulay matrix.

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System ( \rightarrow ) grevlex GB ( \rightarrow ) lex GB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>( O \left( \binom{n + d_{\text{reg}}}{d_{\text{reg}}}^{\omega} \right) ) ( \rightarrow ) ( O(n \cdot #\text{Sol}^\omega) )</td>
</tr>
</tbody>
</table>
Complexity of Gröbner bases computations

Two main indicators of the complexity

- **Degree of regularity** $d_{\text{reg}}$
  \( \leadsto \) degree that has to be reached to compute the grevlex GB.

- **Degree of the ideal** $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$
  \( \leadsto \) number of solutions of the system (counted with multiplicities). Gives the rank of the Macaulay matrix.

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System $\rightarrow$ grevlex GB $\rightarrow$ lex GB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O \left( \left( \begin{array}{c} n + d_{\text{reg}} \ d_{\text{reg}} \end{array} \right) \omega \right)$</td>
</tr>
</tbody>
</table>

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**: $d_{\text{reg}} \leq 1 + \sum_{1 \leq i \leq n} (d_i - 1)$.

- **Bézout bound**: $\deg(\langle f_1, \ldots, f_n \rangle) \leq \prod_{1 \leq i \leq n} d_i$. 
**Complexity of Gröbner bases computations**

**Two main indicators of the complexity**

- **Degree of regularity** $d_{\text{reg}}$
  - degree that has to be reached to compute the **grevlex GB**.

- **Degree of the ideal** $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$
  - Number of solutions of the system (counted with multiplicities). Gives the **rank** of the Macaulay matrix.

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System $\rightarrow$ grevlex GB $\rightarrow$ lex GB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O\left(\left(\frac{n + d_{\text{reg}}}{d_{\text{reg}}}\right)^{\omega}\right)$</td>
</tr>
</tbody>
</table>

**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**: $d_{\text{reg}} \leq 1 + \sum_{1 \leq i \leq n} (d_i - 1)$.

- **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 systems

Multi-homogeneous polynomial

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

\[ f(\lambda_1 X^{(1)}, \ldots, \lambda_\ell X^{(\ell)}) = \lambda_1^{d_1} \ldots \lambda_\ell^{d_\ell} f(X^{(1)}, \ldots, X^{(\ell)}). \]
Multi-homogeneous systems

**Multi-homogeneous polynomial**

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

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

**Example:**

$$3x_1^2 y_1 + 4x_1x_2 y_1 - 3x_2^2 y_1 - x_1^2 y_2 + 8x_1x_2 y_2 - 5x_2^2 y_2 + 10x_1^2 y_3 - 2x_1x_2 y_3 - 3x_2^2 y_3$$

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 systems

**Multi-homogeneous polynomial**

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

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

**Example:**

$$3x_1^2y_1 + 4x_1x_2y_1 - 3x_2^2y_1 - x_1^2y_2 + 8x_1x_2y_2 - 5x_2^2y_2 + 10x_1^2y_3 - 2x_1x_2y_3 - 3x_2^2y_3$$

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)**

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

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

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

\[ f_k = \sum_{i,j} a_{i,j}^{(k)} x_i y_j. \]
Euler relations

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

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

\[ f_k = \sum_i \frac{\partial f_k}{\partial x_i} x_i = \sum_j \frac{\partial f_k}{\partial y_j} y_j. \]
Structure of bilinear systems

**Euler relations**

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

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

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

\[
\begin{bmatrix}
\frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_{n_1}} \\
\vdots & \ddots & \vdots \\
\frac{\partial f_q}{\partial x_1} & \cdots & \frac{\partial f_q}{\partial x_{n_1}}
\end{bmatrix}
\begin{bmatrix}
\frac{\partial f_1}{\partial y_1} & \cdots & \frac{\partial f_1}{\partial y_{n_1}} \\
\vdots & \ddots & \vdots \\
\frac{\partial f_q}{\partial y_1} & \cdots & \frac{\partial f_q}{\partial y_{n_1}}
\end{bmatrix}
\]

\[
\begin{bmatrix}
f_1 \\
\vdots \\
f_q
\end{bmatrix}
= \text{jac}_x(F) \cdot
\begin{bmatrix}
x_1 \\
\vdots \\
x_{n_x}
\end{bmatrix}
= \text{jac}_y(F) \cdot
\begin{bmatrix}
y_1 \\
\vdots \\
y_{n_y}
\end{bmatrix}
\]
When minors...\[ (f_1) \vdots (f_q) = \text{jac}_x(F) \cdot (x_1) \vdots (x_{n_x}) \].

If \((x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y})\) is a non-trivial solution of \(F\), then \(\text{jac}_x(F)\) is rank defective. \(\approx (y_1, \ldots, y_{n_y})\) is a zero of the maximal minors of \(\text{jac}_x(F)\).
Something special happens with minors...

\[
\begin{pmatrix}
  f_1 \\
  \vdots \\
  f_q
\end{pmatrix}
= \text{jac}_x(F) \cdot 
\begin{pmatrix}
  x_1 \\
  \vdots \\
  x_n_x
\end{pmatrix}.
\]

If \((x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y})\) is a non-trivial solution of \(F\), then \(\text{jac}_x(F)\) is rank defective. \(\leadsto (y_1, \ldots, y_{n_y})\) is a zero of the maximal minors of \(\text{jac}_x(F)\).

---

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...

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

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

\(\leadsto (y_1, \ldots, y_{n_y})\) is a zero of the maximal minors of \(\text{jac}_x(F)\).

---

**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 \(<\text{Minors}(M)\>): linear combination of the generators.

\(\leadsto d_{\text{reg}} (\text{MaxMinors}(\text{jac}_x(F))) = n_x\).
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

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

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

$$\min(n_x, n_y) + 1 \ll n_x + n_y + 1.$$
Affine bilinear polynomial

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

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

Degree of regularity

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

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

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** !!

Faugère/Safey El Din/S., J. of Symb. Comp. 2011
Based on **alternant codes**:

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

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

  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.
Based on **alternant codes**:

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

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

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

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

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 \( H \cdot G^t = 0 \) !!

\[
\forall i, j, \quad g_{i,0} y_0 x_j^i + \cdots + g_{i,n-1} y_{n-1} x_{n-1}^i = 0.
\]

\( \Rightarrow \) **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_

⇒ add *redundancy* to the polynomial system
⇔ linear equations ⇔ 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

⇒ add **redundancy** to the polynomial system

⇝ linear equations ⇝ less variables.

Moreover, the system is still over-determined and one can extract a subsystem containing only **powers of two**:

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

⇒ add redundancy to the polynomial system

⇒ linear equations ⇒ less variables.

Moreover, the system is still over-determined and one can extract a subsystem containing only powers of two:

\[ \forall i, j \text{ a power of two } \], \[ g_{i,0} y_0 x_0^j + \cdots + g_{i,n-1} y_{n-1} x_{n-1}^j = 0. \]

Decomposing the subsystem over the field \( \mathbb{F}_2 \)

⇒ **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**

⇒ add **redundancy** to the polynomial system

⇒ linear equations ⇒ less variables.

Moreover, the system is still over-determined and one can extract a subsystem containing only **powers of two**:

\[ \forall i, j \text{ a power of two }!!, \quad g_{i,0}y_0x_j^i + \cdots + g_{i,n-1}y_{n-1}x_j^{n-1} = 0. \]

Decomposing the subsystem over the field \( \mathbb{F}_2 \)

⇒ **Bilinear system with** \( n_x \ll n_y \) !!

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

1. Polynomial System Solving using Gröbner Bases

2. Bilinear Systems and Application to McEliece

3. Determinantal Systems and Applications to MinRank and HFE
The \textit{MinRank} problem

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

\textit{MinRank}

find \( \lambda_1, \ldots, \lambda_k \) such that

\[ \text{Rank} \left( M_0 - \sum_{i=1}^{k} \lambda_i M_i \right) \leq r. \]

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

- Buss, Frandsen, Shallit.
  The computational complexity of some problems of linear algebra.
Two algebraic modelings

\[ M = M_0 - \sum_{i=1}^{k} \lambda_i M_i. \]
Two algebraic modelings

\[ \mathbf{M} = \mathbf{M}_0 - \sum_{i=1}^{k} \lambda_i \mathbf{M}_i. \]

The minors modeling

\[ \text{Rank}(\mathbf{M}) \leq r \]

\[ \Leftrightarrow \text{all minors of size } (r + 1) \text{ of } \mathbf{M} \text{ vanish.} \]

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

Few variables, lots of equations, high degree!!
### Two algebraic modelings

\[ M = M_0 - \sum_{i=1}^{k} \lambda_i M_i. \]

#### The minors modeling

\[ \text{Rank} (M) \leq r \]

- all minors of size \((r + 1)\) of \(M\) vanish.

- \((\begin{pmatrix} m \\ r+1 \end{pmatrix})^2\) equations of degree \(r + 1\).

- \(k\) variables.

Few variables, lots of equations, high degree !!

#### The Kipnis-Shamir modeling

\[ \text{Rank} (M) \leq r \iff \exists x^{(1)}, \ldots, x^{(m-r)} \in \text{Ker}(M). \]

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

- \(m(m - r)\) bilinear equations.

- \(k + r(m - r)\) variables.
Two algebraic modelings

\[ M = M_0 - \sum_{i=1}^{k} \lambda_i M_i. \]

The minors modeling

\[ \text{Rank}(M) \leq r \]

\[ \iff \quad \text{all minors of size } (r+1) \text{ of } M \text{ vanish.} \]

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

Few variables, lots of equations, high degree !!

The Kipnis-Shamir modeling

\[ \text{Rank}(M) \leq r \iff \exists x^{(1)}, \ldots, x^{(m-r)} \in \text{Ker}(M). \]

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

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

- Complexity of solving MinRank using Gröbner bases techniques ?
- Comparison of the two modelings ?
- Number of solutions ?
<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System</th>
<th>grevlex GB</th>
<th>Change of Ordering</th>
<th>lex GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O\left(\binom{n + d_{\text{reg}}}{d_{\text{reg}}}\right)^{\omega}$</td>
<td>$O\left(n \cdot #\text{Sol}^{\omega}\right)$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Main results
Main results

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System</th>
<th>grevlex GB</th>
<th>Change of Ordering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O \left( \left( n + d_{\text{reg}} \right)^{\omega} \right)$</td>
<td>$O (n \cdot #\text{Sol}^{\omega})$</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Modeling:</th>
<th>Minors</th>
<th>Kipnis-Shamir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of regularity when $k = (m - r)^2$</td>
<td>Macaulay bound: $\leq m(m - r) + 1$</td>
<td></td>
</tr>
<tr>
<td>$#\text{Sol}$</td>
<td>MH. Bézout: $\leq \binom{m}{r}^{m-r}$</td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Main results

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System</th>
<th>grevlex GB</th>
<th>Change of Ordering</th>
<th>lex GB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O\left(\left(\frac{n + d_{\text{reg}}}{d_{\text{reg}}}\right)^{\omega}\right)$</td>
<td>$O\left(n \cdot #\text{Sol}^{\omega}\right)$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Modeling:</th>
<th>Minors</th>
<th>Kipnis-Shamir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of regularity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>when $k = (m - r)^2$</td>
<td>$\leq (m - r)^2 + 1$</td>
<td></td>
</tr>
<tr>
<td># Sol</td>
<td>MH. Bézout: $\leq \binom{m}{r}^{m-r}$</td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Main results

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System $\xrightarrow{\text{grevlex GB}}$</th>
<th>Change of Ordering $\xrightarrow{\text{lex GB}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O \left( \left( \frac{n + d_{\text{reg}}}{d_{\text{reg}}} \right)^\omega \right)$</td>
<td>$O(n \cdot #\text{Sol}^\omega)$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Modeling:</th>
<th>Minors</th>
<th>Kipnis-Shamir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of regularity when $k = (m - r)^2$</td>
<td>$r(m - r) + 1$</td>
<td>$\leq (m - r)^2 + 1$</td>
</tr>
<tr>
<td>$#\text{ Sol}$</td>
<td></td>
<td>$\leq \binom{m}{r}^{m-r}$</td>
</tr>
<tr>
<td>Complexity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MH. Bézout: $\leq \binom{m}{r}^{m-r}$
Main results

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System $\rightarrow$ grevlex GB $\rightarrow$ lex GB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O\left((n + d_{\text{reg}})^{\omega}\right)$ $\rightarrow$ $O(n \cdot #\text{Sol}^{\omega})$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Modeling:</th>
<th>Minors</th>
<th>Kipnis-Shamir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of regularity when $k = (m - r)^2$</td>
<td>$r(m - r) + 1$</td>
<td>$\leq (m - r)^2 + 1$</td>
</tr>
<tr>
<td>$#\text{Sol}$</td>
<td>$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$</td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Main results

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System $\rightarrow$ grevlex GB $\rightarrow$ lex GB.</th>
<th>Change of Ordering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O\left(\left(\begin{array}{c} n + d_{\text{reg}} \ d_{\text{reg}} \end{array}\right)^{\omega}\right)$</td>
<td>$O\left(n \cdot #\text{Sol}^{\omega}\right)$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Modeling:</th>
<th>Minors</th>
<th>Kipnis-Shamir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of regularity when $k = (m - r)^2$</td>
<td>$r(m - r) + 1$</td>
<td>$\leq (m - r)^2 + 1$</td>
</tr>
<tr>
<td>$#\text{Sol}$</td>
<td>$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$</td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>$O(m^{\omega k})$</td>
<td>$O(m^{\omega(k+1)})$</td>
</tr>
</tbody>
</table>
Main results

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>System $\rightarrow$ grevlex GB $\rightarrow$ lex GB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>$O\left(\left(\frac{n + d_{reg}}{d_{reg}}\right)^{\omega}\right)$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Modeling:</th>
<th>Minors</th>
<th>Kipnis-Shamir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of regularity when $k = (m - r)^2$</td>
<td>$r(m - r) + 1$</td>
<td>$\leq (m - r)^2 + 1$</td>
</tr>
<tr>
<td>$#\text{Sol}$</td>
<td>$\prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}$</td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>$O(m^{\omega k})$</td>
<td>$O(m^{\omega(k+1)})$</td>
</tr>
</tbody>
</table>

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

**New Crypto challenge broken:** 10 generic matrices of size $11 \times 11$ target rank 8, $K = \text{GF}(65521)$. 
*Courtois, Asiacrypt 2001.*
Minors modeling:

\[
\text{Rank}(M) \leq r \\
\Leftrightarrow \\
\text{all minors of size } (r + 1) \text{ of } M \text{ vanish.}
\]

\[\leadsto \text{Determinantal ideal}\]
Minors modeling:

\[ \text{Rank}(M) \leq r \]

\[ \iff \]

all minors of size \((r + 1)\) of \(M\) vanish.

\[ \hookrightarrow \text{Determinantal ideal} \]

**Bilinear systems \(\leftrightarrow\) determinantal systems**

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

\[
\begin{pmatrix}
\frac{\partial f_1}{\partial x_0} & \ldots & \frac{\partial f_1}{\partial x_{nx}} \\
\vdots & \ddots & \vdots \\
\frac{\partial f_q}{\partial x_0} & \ldots & \frac{\partial f_q}{\partial x_{nx}}
\end{pmatrix}
\cdot
\begin{pmatrix}
x_0 \\
\vdots \\
x_{nx}
\end{pmatrix}
= 
\begin{pmatrix}
f_1 \\
\vdots \\
f_q
\end{pmatrix}
\]

\[ f_1 = \ldots = f_q = 0 \iff \text{MaxMinors (Jac}_X(f_1, \ldots, f_q)) = 0. \]
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

\[ \mathcal{D} = \text{Minors}_{r+1} \left( \begin{array}{ccc} v_{1,1} & \cdots & v_{1,m} \\ \vdots & \ddots & \vdots \\ v_{m,1} & \cdots & v_{m,m} \end{array} \right) \]

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

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

\[
A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell} \binom{m-j}{\ell} t^\ell.
\]
Properties of Determinantal Ideals

\[ D = \text{Minors}_{r+1} \left( \begin{array}{ccc}
v_{1,1} & \ldots & v_{1,m} \\
\vdots & \ddots & \vdots \\
v_{m,1} & \ldots & v_{m,m}
\end{array} \right) \]

\[ I = \text{Minors}_{r+1} \left( \begin{array}{ccc}
f_{1,1} & \ldots & f_{1,m} \\
\vdots & \ddots & \vdots \\
f_{m,1} & \ldots & f_{m,m}
\end{array} \right) \]

The degree of \( D \) is

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

The Hilbert series of \( D \) is

\[
\text{HS}_D(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{2m-r}r^r}.
\]

\[
A_{i,j}(t) = \sum_{\ell} \binom{m-i}{\ell} \binom{m-j}{\ell} t^\ell.
\]
properties of determinantal ideals

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

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

The degree of \( D \) is

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

Conca/Herzog, Abhyankar

The Hilbert series of \( D \) is

\[ \text{HS}_D(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}(1-t)^{2m-r}r}. \]

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

Transfer of properties of \( D \) by adding \( \langle v_{i,j} - f_{i,j} \rangle \).
### Properties of Determinantal Ideals

Let \( \mathcal{D} = \text{Minors}_{r+1} \left( \begin{array}{ccc} v_{1,1} & \ldots & v_{1,m} \\ \vdots & \ddots & \vdots \\ v_{m,1} & \ldots & v_{m,m} \end{array} \right) \)

**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

\[
HS_{\mathcal{D}}(t) = \frac{\det(A(t))}{t^{{m-r}}} \frac{1}{(1-t)^{(2m-r)r}}.
\]

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

**ISSAC’2010**

Let \( \mathcal{I} = \text{Minors}_{r+1} \left( \begin{array}{ccc} f_{1,1} & \ldots & f_{1,m} \\ \vdots & \ddots & \vdots \\ f_{m,1} & \ldots & f_{m,m} \end{array} \right) \)

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

\[
HS_{\mathcal{I}}(t) = \frac{\det(A(t))}{t^{{m-r}}} \frac{1}{(1-t)^{(m-r)^2}}.
\]

**transfer of properties of \( \mathcal{D} \) by adding** \( \langle v_{i,j} - f_{i,j} \rangle \)
Degree of regularity for a 0-dim ideal $= 1 + \text{degree of the Hilbert series}$.

**Corollary**

The degree of regularity of $I$ is generically equal to

$$d_{\text{reg}} = r(m - r) + 1.$$
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

$$d_{\text{reg}} = r(m - r) + 1.$$  

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

$$O(m^{\omega k}).$$
Corollary: generic number of solutions

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

\[
\#Sol = m - r - 1 \prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}
\]

\[
\sim m \rightarrow \infty \quad m^k \prod_{i=0}^{m-r-1} \frac{i!}{(m-r+i)!}.
\]
Corollary: generic number of solutions

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

\[
\#\text{Sol} = \prod_{i=0}^{m-r-1} \frac{i!(m+i)!}{(m-1-i)!(m-r+i)!}
\]

\[
\sim m^k \prod_{i=0}^{m-r-1} \frac{i!}{(m-r+i)!}.
\]

Complexity of the Change of Ordering (ISSAC 2010)

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

\[
O(\#\text{Sol}^\omega) = O\left(m^{\omega k}\right).
\]
Efficient zero-knowledge authentication based on a linear algebra problem MinRank.

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

<table>
<thead>
<tr>
<th>Challenge</th>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(6, 9, 3)</td>
<td>(7, 9, 4)</td>
<td>(8, 9, 5)</td>
</tr>
<tr>
<td>degree</td>
<td>980</td>
<td>4116</td>
<td>14112</td>
</tr>
</tbody>
</table>

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  | \(\infty\) |
| F_5 mem   | 407 MB   | 3113 MB  | 58587 MB |          |
| log_2(Nb op.) | 30.5 | 37.1 | 43.4 |
| FGLM time | 35s      | 2580s    | \(\infty\) |
Experimental results

Courtois. Asiacrypt’01.

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

\[ K = \text{GF}(65521) \quad (m, k, r): \quad k \text{ matrices of size } m \times m. \text{ Target rank: } r. \]

<table>
<thead>
<tr>
<th>Challenge</th>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(6, 9, 3)</td>
<td>(7, 9, 4)</td>
<td>(8, 9, 5)</td>
</tr>
<tr>
<td>degree</td>
<td>980</td>
<td>4116</td>
<td>14112</td>
</tr>
</tbody>
</table>

Minors modeling

<table>
<thead>
<tr>
<th></th>
<th>(d_{\text{reg}})</th>
<th>(F_5) time</th>
<th>(F_5) mem</th>
<th>(\log_2(\text{Nb op.}))</th>
<th>FGLM time</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10</td>
<td>1.1s</td>
<td>488 MB</td>
<td>21.5</td>
<td>0.5s</td>
</tr>
<tr>
<td>B</td>
<td>13</td>
<td>28.4s</td>
<td>587 MB</td>
<td>25.9</td>
<td>28.5s</td>
</tr>
<tr>
<td>C</td>
<td>16</td>
<td>544s</td>
<td>1213 MB</td>
<td>29.2</td>
<td>1033s</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>9048s</td>
<td>5048 MB</td>
<td>32.7</td>
<td>22171s</td>
</tr>
</tbody>
</table>

Kipnis-Shamir modeling

<table>
<thead>
<tr>
<th></th>
<th>(d_{\text{reg}})</th>
<th>(F_5) time</th>
<th>(F_5) mem</th>
<th>(\log_2(\text{Nb op.}))</th>
<th>FGLM time</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>5</td>
<td>30s</td>
<td>407 MB</td>
<td>30.5</td>
<td>35s</td>
</tr>
<tr>
<td>B</td>
<td>6</td>
<td>3795s</td>
<td>3113 MB</td>
<td>37.1</td>
<td>2580s</td>
</tr>
<tr>
<td>C</td>
<td>7</td>
<td>328233s</td>
<td>58587 MB</td>
<td>43.4</td>
<td>∞</td>
</tr>
</tbody>
</table>

Computational bottleneck: computing the minors.

Computing effort needed for solving Challenge C:

238 days on 64 quadricore processors.
Algebraic cryptanalysis of \((\text{multi-})\text{HFE}\)

Patarin, Eurocrypt’96
Billet/Patarin/Seurin, ICSCC’08

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

\[ \leadsto \text{low-rank quadratic form } (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n \]
Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt’96
Billet/Patarin/Seurin, ICSCC’08

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

\( \rightsquigarrow \textbf{low-rank} \text{ quadratic form } (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n \)

masked by \textbf{linear transforms} !!
Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt’96
Billet/Patarin/Seurin, ICSCC’08

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

\( \leadsto \) low-rank quadratic form \((\mathbb{F}_{q})^n \rightarrow (\mathbb{F}_{q})^n\) 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

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

\( \leadsto \) algebraic attack with polynomial complexity in \( n !! \)

\( \leadsto \) attacks on odd-characteristic variants;

\( \leadsto \) generalizations to multi-HFE.
Structures have an impact on the complexity of the solving process in algebraic cryptanalysis!

Design, key size reduction, ... Structure $\leftrightarrow$ potential algebraic attacks.
Conclusion and Perspectives

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

Design, key size reduction, \( \leftrightarrow \) 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).
Conclusion and Perspectives

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

Design, key size reduction, ... \(\leftrightarrow\) 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.
  \(\sim\) (Faugère, Safey, S., J. of Symb. Comp. 2011)
- Dedicated algorithm for **determinantal systems**?