

Résolution de systèmes polynomiaux structurés et applications en Cryptologie

Pierre-Jean Spaenlehauer

University of Western Ontario – Ontario Research Center for Computer Algebra

Magali Bardet, Jean-Charles Faugère,
Mohab Safey El Din, Bruno Salvy

Séminaire CAMEL, LORIA
17/01/2013

0-dimensional polynomial systems in applications

$$f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n],$$

where \mathbb{K} is a field

$$\left\{ \begin{array}{l} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{array} \right. \quad \left. \begin{array}{l} \text{list the solutions in} \\ \overline{\mathbb{K}}^n \\ \mathbb{K}^n \\ \mathbb{R}^n \end{array} \right.$$

0-dimensional polynomial systems in applications

$$f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n],$$

where \mathbb{K} is a field

$$\left\{ \begin{array}{l} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{array} \right. \quad \left. \begin{array}{l} \text{list the solutions in} \\ \overline{\mathbb{K}}^n \\ \mathbb{K}^n \\ \mathbb{R}^n \end{array} \right.$$

NP-hard problem when \mathbb{K} is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

0-dimensional polynomial systems in applications

$$f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n], \quad \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases} \quad \begin{array}{l} \text{list the solutions in} \\ \mathbb{K}^n \\ \mathbb{K}^n \\ \mathbb{R}^n \end{array}$$

where \mathbb{K} is a field

NP-hard problem when \mathbb{K} is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

Methods and algorithms

- Homotopy (symbolic/numeric)
- Geometric resolution
- Triangular sets
- **Gröbner bases**
 \rightsquigarrow adapted to every field

0-dimensional polynomial systems in applications

$$f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n], \quad \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases} \quad \begin{array}{l} \text{list the solutions in} \\ \mathbb{K}^n \\ \mathbb{K}^n \\ \mathbb{R}^n \end{array}$$

where \mathbb{K} is a field

NP-hard problem when \mathbb{K} is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

Methods and algorithms

- Homotopy (symbolic/numeric)
- Geometric resolution
- Triangular sets
- **Gröbner bases**
 \rightsquigarrow adapted to every field

Algebraic cryptanalysis

- Algebraic **modeling** of cryptographic primitives
- **Finite elds**
- Complexity analysis
 \rightsquigarrow **Security estimates**

0-dimensional polynomial systems in applications

$$f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n], \quad \text{where } \mathbb{K} \text{ is a field} \quad \left\{ \begin{array}{l} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{array} \right. \quad \begin{array}{l} \text{list the solutions in} \\ \mathbb{K}^n \\ \mathbb{K}^n \\ \mathbb{R}^n \end{array}$$

NP-hard problem when \mathbb{K} is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

Methods and algorithms

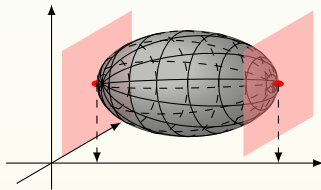
- Homotopy (symbolic/numeric)
- Geometric resolution
- Triangular sets
- **Gröbner bases**
 \rightsquigarrow adapted to every field

Algebraic cryptanalysis

- Algebraic **modeling** of cryptographic primitives
- **Finite elds**
- Complexity analysis
 \rightsquigarrow **Security estimates**

Real geometry and Optimization

- Field of **rationals**
- **Critical point** method
- **Optimization** under polynomial constraints



0-dimensional polynomial systems in applications

$$f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n], \quad \text{where } \mathbb{K} \text{ is a field} \quad \left\{ \begin{array}{l} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{array} \right. \quad \begin{array}{l} \text{list the solutions in} \\ \mathbb{K}^n \\ \mathbb{K}^n \\ \mathbb{R}^n \end{array}$$

NP-hard problem when \mathbb{K} is finite (**Bézout theorem** $\rightsquigarrow d^n$ solutions).

Methods and algorithms

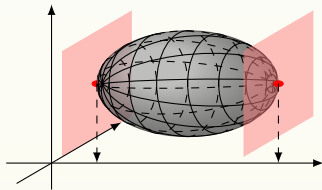
- Homotopy (symbolic/numeric)
- Geometric resolution
- Triangular sets
- **Gröbner bases**
 \rightsquigarrow adapted to every field

Algebraic cryptanalysis

- Algebraic **modeling** of cryptographic primitives
- **Finite elds**
- Complexity analysis
 \rightsquigarrow **Security estimates**

Real geometry and Optimization

- Field of **rationals**
- **Critical point** method
- **Optimization** under polynomial constraints



My Ph.D. thesis: impact of structures in GB computations

Challenges for Structured systems – Motivations

Less solutions than a dense system. Experimentally, **easier** to solve.

Challenges for Structured systems – Motivations

Less solutions than a dense system. Experimentally, **easier** to solve.

Structure	number of solutions	example
dense bilinear	$2^{n_x+n_y}$ $\binom{n_x+n_y}{n_x}$	$n_x = 9, n_y = 3$ 4 096 84
dense determinantal	$(r+1)^{(p-r)(q-r)}$ $\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$	$r = 8, p = 11, q = 12$ 282 429 536 481 4 723 719

Challenges for Structured systems – Motivations

Less solutions than a dense system. Experimentally, easier to solve.

Structure	number of solutions	example
dense bilinear	$2^{n_x+n_y}$ $\binom{n_x+n_y}{n_x}$	$n_x = 9, n_y = 3$
		4 096 84
dense determinantal	$(r+1)^{(p-r)(q-r)}$ $\prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$	$r = 8, p = 11, q = 12$
		282 429 536 481 4 723 719

Critical questions

- **Complexity?**: polynomial in the number of solutions? polynomial in the number of variables?
- **Dedicated algorithms?**: how to exploit the structures to obtain efficient solving techniques?
- **Validation and Applications?**: which structures? systematic methods of analysis? experimental validation (asymptotic vs. practical complexity)?

0-dimensional solving strategy

$$f_1 = \dots = f_m = 0$$

+

“grevlex” Gb

Row Echelon forms of **Macaulay matrices** up to degree d_{reg}

$$O\left(m \binom{n+d_{\text{reg}}}{n}^\omega\right)$$

+

“lex” Gb

Linear algebra in $\frac{\mathbb{K}[X]}{I}$ as a \mathbb{K} -
vect. space of dim. $\text{DEG}(I)$
 $\rightsquigarrow g(u) = 0, x_i = h_i(u)$

$$O(n \text{DEG}(I)^3)$$

Complexity

Algorithms

Buchberger (1965)

F_4 (**Faugère 1999**)

F_5 (**Faugère 2002**)

FGLM

Faugère, Gianni,

Lazard, Mora (1993)

0-dimensional solving strategy

$$f_1 = \dots = f_m = 0$$

+

“grevlex” Gb

Row Echelon forms of **Macaulay matrices** up to degree d_{reg}

Complexity

$$O\left(m \binom{n+d_{\text{reg}}}{n}^\omega\right)$$

Algorithms

Buchberger (1965)
 F_4 (Faugère 1999)
 F_5 (Faugère 2002)

+

“lex” Gb

Linear algebra in $\frac{\mathbb{K}[X]}{I}$ as a \mathbb{K} -
 vect. space of dim. $\text{DEG}(I)$
 $\rightsquigarrow g(u) = 0, x_i = h_i(u)$

$$O(n \text{DEG}(I)^3)$$

FGLM

Faugère, Gianni,
 Lazard, Mora (1993)

Macaulay matrix in degree d

$$f_1 = \dots = f_p = 0, \deg(f_i) = d_i$$

Rows: all products tf_i where
 $t \geq \text{Monomials}(d - d_i)$.

Columns: monomials of degree d .

$$\begin{matrix} t_1 f_1 \\ \vdots \\ t_k f_p \end{matrix} \begin{pmatrix} m_1 & & m_\ell \\ & & \end{pmatrix}$$

0-dimensional solving strategy

$$f_1 = \dots = f_m = 0$$

- 1 Introduction
- 2 MinRank
 - 1 Determinantal ideals
 - 2 Multi-homogeneous systems
 - 3 Applications in Cryptology
- 3 Quadratic boolean systems

1 Introduction

2 MinRank

- 1 Determinantal ideals
- 2 Multi-homogeneous systems
- 3 Applications in Cryptology

3 Quadratic boolean systems

The MinRank problem

$r \geq 2 \in \mathbb{N}$. M_0, \dots, M_n : $n + 1$ matrices of size $q \times q$.

MinRank

find $\lambda_1, \dots, \lambda_n$ such that

$$\text{Rank} \left(M_0 + \sum_{i=1}^n \lambda_i M_i \right) \leq r$$

The MinRank problem

$r \in \mathbb{N}$. M_0, \dots, M_n : $n + 1$ matrices of size $q \times q$.

MinRank

find $\lambda_1, \dots, \lambda_n$ such that

$$\text{Rank} \left(M_0 + \sum_{i=1}^n \lambda_i M_i \right) \leq r$$

- **Multivariate** generalization of the **EigenValue** problem.
- Applications in **cryptology**, **coding theory**, **geometry**, ...
Kipnis/Shamir Crypto'99
Courtois Crypto'01
- Fundamental **NP-hard** problem of **linear algebra**.



Buss, Frandsen, Shallit.

J. of Computer and System Sciences. 1999.

The computational complexity of some problems of linear algebra.

Two algebraic modelings

$$\mathbf{M} = M_0 + \sum_{i=1}^n \lambda_i M_i,$$

\mathbf{q} : size of the matrices, \mathbf{r} : target rank

$$\mathbf{M} = M_0 + \sum_{i=1}^n \lambda_i M_i,$$

q : size of the matrices, r : target rank

The minors modeling

$$\text{Rank}(\mathbf{M}) \leq r$$



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

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

Few variables, lots of equations, high degree !!

Two algebraic modelings

$$\mathbf{M} = M_0 + \sum_{i=1}^n \lambda_i M_i,$$

q : size of the matrices, r : target rank

The minors modeling

$$\text{Rank}(\mathbf{M}) \leq r$$



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

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

Few **variables**, lots of **equations**, high **degree** !!

The Kipnis-Shamir modeling

$$\text{Rank}(\mathbf{M}) = r, \quad \exists x^{(1)}, \dots, x^{(q-r)} \in \text{Ker}(\mathbf{M}).$$

$$\mathbf{M} \begin{pmatrix} I_{q-r} \\ x_1^{(1)} \quad \dots \quad x_1^{(q-r)} \\ \vdots \quad \quad \quad \vdots \\ x_r^{(1)} \quad \dots \quad x_r^{(q-r)} \end{pmatrix} = 0$$

- $q(q-r)$ **bilinear** equations.
- $n + r(q-r)$ variables.

Two algebraic modelings

$$\mathbf{M} = M_0 + \sum_{i=1}^n \lambda_i M_i,$$

q : size of the matrices, r : target rank

The minors modeling

$$\text{Rank}(\mathbf{M}) \leq r$$



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

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

Few **variables**, lots of **equations**, high **degree** !!

The Kipnis-Shamir modeling

$$\text{Rank}(\mathbf{M}) = r, \quad \exists x^{(1)}, \dots, x^{(q-r)} \in \text{Ker}(\mathbf{M}).$$

$$\mathbf{M} \begin{pmatrix} I_{q-r} \\ x_1^{(1)} \quad \dots \quad x_1^{(q-r)} \\ \vdots \quad \quad \quad \vdots \\ x_r^{(1)} \quad \dots \quad x_r^{(q-r)} \end{pmatrix} = 0$$

- $q(q-r)$ **bilinear** equations.
- $n + r(q-r)$ variables.

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



Faugère, Levy-dit-Vehel, Perret.

Crypto '08.

Cryptanalysis of MinRank.

	System	!	grevlex GB	!	lex GB.
<i>Complexity</i>				Change of ordering	
	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$				$O(n \#Sol^3)$



Faugère, Levy-dit-Vehel, Perret.

Crypto '08.

Cryptanalysis of MinRank.

	System	!	grevlex GB	!	lex GB.
<i>Complexity</i>	$O\left(\binom{n}{q}^2 \binom{n + d_{\text{reg}}}{d_{\text{reg}}}\right)$			Change of ordering	$O(n \#Sol^3)$

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$		$d_{\text{reg}} = q(q - r) + 1$
# Sol		$< \binom{q}{r}^{q-r}$
Complexity		polynomial in q when n is fixed ?

1 Introduction

2 **MinRank**

1 **Determinantal ideals**

2 Multi-homogeneous systems

3 Applications in Cryptology

3 Quadratic boolean systems

Let $r < q < p$ be integers and M be the $p \times q$ matrix

$$M = \begin{bmatrix} f_{1,1} & & f_{1,q} \\ \vdots & & \vdots \\ f_{p,1} & & f_{p,q} \end{bmatrix}$$

with $f_{i,j} \in \mathbb{K}[x_1, \dots, x_n]$ of **degree D** .

The **evaluation** of M at $\mathbf{x} \in \overline{\mathbb{K}}^n$ is denoted by $M_{\mathbf{x}}$.

Determinantal systems

Let $r < q < p$ be integers and M be the $p \times q$ matrix

$$M = \begin{bmatrix} f_{1,1} & \dots & f_{1,q} \\ \vdots & & \vdots \\ f_{p,1} & \dots & f_{p,q} \end{bmatrix}$$

with $f_{i,j} \in \mathbb{K}[x_1, \dots, x_n]$ of degree D .

The **evaluation** of M at $\mathbf{x} \in \overline{\mathbb{K}}^n$ is denoted by $M_{\mathbf{x}}$.

Generalized MinRank Problem

Describe the set $V \subseteq \overline{\mathbb{K}}^n$ of points $\mathbf{x} \in \overline{\mathbb{K}}^n$ such that $\text{rank}(M_{\mathbf{x}}) = r$.

\rightsquigarrow **polynomial system solving** problem: $\text{Minors}_{r+1}(M) = 0$

Main results (ISSAC 2010 + generalization submitted)

with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D .

	System	!	grevlex GB	!	lex GB.
<i>Complexity</i>	$O\left(\binom{p}{r+1} \binom{q}{r+1} \binom{n + d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$			Change of ordering	$O(n \cdot \#\text{Sol}^3)$

Main results (ISSAC 2010 + generalization submitted)

with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D .

	System	!	grevlex GB	!	lex GB.
<i>Complexity</i>	$O\left(\binom{p}{r+1} \binom{q}{r+1} \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)$			Change of ordering	$O(n \cdot \#\text{Sol}^3)$

Zero-dimensional case ($n = (p - r)(q - r)$)

New bounds under genericity assumptions

$$d_{\text{reg}} = Dr(q - r) + (D - 1)(p - r)(q - r) + 1 < (pD - 1)(p - r)(q - r) + 1$$

Main results (ISSAC 2010 + generalization submitted)

with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D .

	System	!	grevlex GB	!	lex GB.
<i>Complexity</i>	$O\left(\binom{p}{r+1} \binom{q}{r+1} \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$			Change of ordering	$O(n \cdot \#\text{Sol}^3)$

Zero-dimensional case ($n = (p-r)(q-r)$)

New bounds under genericity assumptions

$$d_{\text{reg}} = Dr(q-r) + (D-1)(p-r)(q-r) + 1 < (pD-1)(p-r)(q-r) + 1$$

$$\#\text{Sol} = D^{(p-r)(q-r)} \prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!} < (pD)^{(p-r)(q-r)}$$

Main results (ISSAC 2010 + generalization submitted)

with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D .

	System	grevlex GB	lex GB.
<i>Complexity</i>	$O\left(\binom{p}{r+1} \binom{q}{r+1} \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)$	$O(n \cdot \text{\#Sol}^3)$	

Zero-dimensional case ($n = (p-r)(q-r)$)

New bounds under genericity assumptions

$$d_{\text{reg}} = Dr(q-r) + (D-1)(p-r)(q-r) + 1 < (pD-1)(p-r)(q-r) + 1$$

$$\#Sol = D^{(p-r)(q-r)} \prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!} < (pD)^{(p-r)(q-r)}$$

- ↪ new **complexity bounds** for the solving the Generalized MinRank Problem;
- ↪ families of Generalized MinRank Problems that can be solved in complexity **polynomial** in the **number of solutions**.

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

Entries are **variables**

$$r \quad r \text{ matrix: } A_{i,j}(t) = \sum_{\ell} \binom{p-i}{\ell} \binom{q-j}{\ell} t^{\ell}$$

Roadmap of the proof

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

Thom/Porteous 71, Giambelli 04,
Harris/Tu 84

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

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

Conca/Herzog AMS'94, Abhyankar '88

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

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

$$r \times r \text{ matrix: } A_{i,j}(t) = \sum_{\ell} \binom{p-i}{\ell} \binom{q-j}{\ell} t^{\ell}$$

Roadmap of the proof

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

Thom/Porteous 71, Giambelli 04,
Harris/Tu 84

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

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

Conca/Herzog AMS'94, Abhyankar '88

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

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

$$r \times r \text{ matrix: } A_{i,j}(t) = \sum_{\ell} \binom{p-i}{\ell} \binom{q-j}{\ell} t^{\ell}$$

$$I = \text{Minors}_{r+1} \begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}$$

Entries are **polynomials**

Roadmap of the proof

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

Thom/Porteous 71, Giambelli 04,
Harris/Tu 84

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

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

Conca/Herzog AMS'94, Abhyankar '88

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

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

$r \times r$ matrix: $A_{i,j}(t) = \sum_{\ell} \binom{p-i}{\ell} \binom{q-j}{\ell} t^{\ell}$

transfer of properties of D by adding

$$hv_{i,j} \quad f_{i,j}$$

$$I = \text{Minors}_{r+1} \begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}$$

Entries are **polynomials**

Roadmap of the proof

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

Thom/Porteous 71, Giambelli 04,
Harris/Tu 84

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

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

Conca/Herzog AMS'94, Abhyankar '88

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

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

$r \times r$ matrix: $A_{i,j}(t) = \sum_{\ell} \binom{p-i}{\ell} \binom{q-j}{\ell} t^{\ell}$

transfer of properties of D by adding

$$hv_{i,j} \quad f_{i,j}$$

$$I = \text{Minors}_{r+1} \begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}$$

The **degree** of I is

$$D^{(p-r)(q-r)} \prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

The **Hilbert series** of I is

$$\text{HS}_{\mathcal{I}}(t) = \frac{\det(A(t^D))(1-t^D)^{(p-r)(q-r)}}{t^{\binom{r}{2}} (1-t)^n}$$

Roadmap of the proof

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

Thom/Porteous 71, Giambelli 04,
Harris/Tu 84

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

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

Conca/Herzog AMS'94, Abhyankar '88

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

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

$r \times r$ matrix: $A_{i,j}(t) = \sum_{\ell} \binom{p-i}{\ell} \binom{q-j}{\ell} t^{\ell}$

transfer of properties of D by adding
 $h_{v_{i,j}} \quad f_{i,j}$

$$I = \text{Minors}_{r+1} \begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}$$

The **degree** of I is

$$D^{(p-r)(q-r)} \prod_{i=0}^{q-r-1} \frac{i!(p+i)!}{(q-1-i)!(p-r+i)!}$$

The **Hilbert series** of I is

$$\text{HS}_{\mathcal{I}}(t) = \frac{\det(A(t^D))(1-t^D)^{(p-r)(q-r)}}{t^{\binom{r}{2}} (1-t)^n}$$

Ingredients of the proof:

- **Cohen-Macaulay** rings;
- **quasi-homogeneous** polynomials.

MinRank – Complexity of the minors modeling

	System	!	grevlex GB	!	lex GB.
<i>Complexity</i>				Change of ordering	

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	$d_{\text{reg}} = q(q - r) + 1$
# Sol		$< \binom{q}{r}^{q-r}$
Complexity		poly(q)??

MinRank – Complexity of the minors modeling

	System	grevlex GB	lex GB.
<i>Complexity</i>	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)$	<i>Change of ordering</i>	$O(n \cdot \#Sol^3)$

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	$d_{\text{reg}} = q(q - r) + 1$
# Sol	$\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$	New $< \binom{q}{r}^{q-r}$
Complexity	$O(q^{3n})$	poly(q)??

Complexity **polynomial** in q ;

MinRank – Complexity of the minors modeling

	System	!	grevlex GB	!	lex GB.
<i>Complexity</i>				Change of ordering	
	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$				$O(n \cdot \#Sol^3)$

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	$d_{\text{reg}} = q(q - r) + 1$
# Sol	$\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$	New $< \binom{q}{r}^{q-r}$
Complexity	$O(q^{3n})$	poly(q)??

Complexity **polynomial** in q ;
Compatible **genericity assumptions**;

1 Introduction

2 **MinRank**

1 Determinantal ideals

2 **Multi-homogeneous systems**

3 Applications in Cryptology

3 Quadratic boolean systems

Relation between bilinear and determinantal systems

$F = (f_1, \dots, f_m) \in \mathbb{K}[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}]^m$: system of **bilinear equations**.

$$\text{jac}_X(F) = \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_0} & \cdots & \frac{\partial f_m}{\partial x_{n_x}} \end{pmatrix} \quad \text{jac}_Y(F) = \begin{pmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{pmatrix}$$

Euler relations

$$f = \sum x_j \frac{\partial f}{\partial x_j} = \sum y_j \frac{\partial f}{\partial y_j}.$$

$$\text{jac}_X(F) \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} \quad \text{jac}_Y(F) \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}$$

Relation between bilinear and determinantal systems

$F = (f_1, \dots, f_m) \in \mathbb{K}[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}]^m$: system of **bilinear equations**.

$$\text{jac}_X(F) = \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_0} & \cdots & \frac{\partial f_m}{\partial x_{n_x}} \end{pmatrix} \quad \text{jac}_Y(F) = \begin{pmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{pmatrix}$$

Euler relations

$$f = \sum x_j \frac{\partial f}{\partial x_j} = \sum y_j \frac{\partial f}{\partial y_j}.$$

$$\text{jac}_X(F) \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} \quad \text{jac}_Y(F) \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}$$

$$f_1 = \cdots = f_m = 0 \implies \text{Minors}_{n_x+1}(\text{jac}_X(F)) = 0$$

Relation between bilinear and determinantal systems

$F = (f_1, \dots, f_m) \in \mathbb{K}[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}]^m$: system of **bilinear equations**.

$$\text{jac}_X(F) = \begin{pmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_0} & \cdots & \frac{\partial f_m}{\partial x_{n_x}} \end{pmatrix} \quad \text{jac}_Y(F) = \begin{pmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{pmatrix}$$

Euler relations

$$f = \sum x_j \frac{\partial f}{\partial x_j} = \sum y_j \frac{\partial f}{\partial y_j}.$$

$$\text{jac}_X(F) \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} \quad \text{jac}_Y(F) \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}$$

$$f_1 = \cdots = f_m = 0 \implies \text{Minors}_{n_x+1}(\text{jac}_X(F)) = 0 \\ \implies d_{\text{reg}} \leq \min(n_x, n_y) + 1.$$

Main results (*J. of Symbolic Computation 2011*)

with J.-C. Faugère, M. Safey El Din

Giusti
Lazard
Macaulay

Bardet
Faugère
Salvy

New results:

	$m \leq n$	$m = \alpha n$	bilinear $m \leq n_x + n_y$
reductions to 0	F_5 criterion		extended F_5 crit.
subclass	regularity	semi-regularity	biregularity
Hilbert series	$\frac{\prod(1 - t^{d_i})}{(1 - t)^n}$	$\left[\frac{\prod(1 - t^{d_i})}{(1 - t)^n} \right]_+$	$\frac{Q(t_1, t_2)}{(1 - t_1)^{n_x}(1 - t_2)^{n_y}}$
complexity	$\approx 2^{\omega n}$	$\approx 2^{\omega(\alpha - 1/2 - \sqrt{\alpha(\alpha - 1)})n}$	$\approx 2^{\omega \min(n_x, n_y)}$

Main results (*J. of Symbolic Computation 2011*)

with J.-C. Faugère, M. Safey El Din

Giusti
Lazard
Macaulay

Bardet
Faugère
Salvy

New results:

	$m \leq n$	$m = \alpha n$	bilinear $m \leq n_x + n_y$
reductions to 0	F_5 criterion		extended F_5 crit.
subclass	regularity	semi-regularity	biregularity
Hilbert series	$\frac{\prod(1-t^{d_i})}{(1-t)^n}$	$\left[\frac{\prod(1-t^{d_i})}{(1-t)^n} \right]_+$	$\frac{Q(t_1, t_2)}{(1-t_1)^{n_x}(1-t_2)^{n_y}}$
complexity	$\approx 2^{\omega n}$	$\approx 2^{\omega(\alpha-1/2-\sqrt{\alpha(\alpha-1)})n}$	$\approx 2^{\omega \min(n_x, n_y)}$

- New theoretical **complexity bounds**. Experimentally observed.
- New classes of **affine bilinear systems** solved in **polynomial time**.

$$\rightsquigarrow \min(n_x, n_y) \text{ bounded} \Rightarrow \begin{cases} \text{poly in } n_x + n_y \\ \text{poly in } \mathbf{nb. solutions.} \end{cases}$$

MinRank – Complexity of Kipnis-Shamir modeling

	System	! grevlex GB	! lex GB.
<i>Complexity</i>	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$	Change of ordering	$O(n \#Sol^3)$

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	$d_{\text{reg}} < q(q - r) + 1$
# Sol		New $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$
Complexity	$O(q^{3n})$	

MinRank – Complexity of Kipnis-Shamir modeling

	System	grevlex GB	lex GB.
<i>Complexity</i>	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$	<i>Change of ordering</i>	$O(n \#Sol^3)$

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	New $d_{\text{reg}} (q - r)^2 + 2 < q(q - r) + 1$
# Sol		New $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$
Complexity	$O(q^{3n})$	

MinRank – Complexity of Kipnis-Shamir modeling

	System	grevlex GB	lex GB.
<i>Complexity</i>	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$	<i>Change of ordering</i>	$O(n \#Sol^3)$

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	New $d_{\text{reg}} (q - r)^2 + 2 < q(q - r) + 1$
# Sol		New $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$
Complexity	$O(q^{3n})$	$O(q^{3(n+2)})$: polynomial in q

MinRank – Complexity of Kipnis-Shamir modeling

	System	! grevlex GB	! lex GB.
<i>Complexity</i>	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$	<i>Change of ordering</i>	$O(n \#Sol^3)$

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	New $d_{\text{reg}} (q - r)^2 + 2 < q(q - r) + 1$
# Sol		New $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$
Complexity	$O(q^{3n})$	$O(q^{3(n+2)})$: polynomial in q

But...

MinRank – Complexity of Kipnis-Shamir modeling

	System	grevlex GB	lex GB.
<i>Complexity</i>	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$	$O(n \cdot \#Sol^3)$	<i>Change of ordering</i>

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	New $d_{\text{reg}} (q - r)^2 + 2 < q(q - r) + 1$
# Sol		New $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$
Complexity	$O(q^{3n})$	$O(q^{3(n+2)})$: polynomial in q

But... different **genericity assumptions** \rightsquigarrow bound not sharp

MinRank – Complexity of Kipnis-Shamir modeling

	System	!	grevlex GB	!	lex GB.
				Change of ordering	
Complexity	$O\left(\binom{n}{q}^2 \binom{n+d_{\text{reg}}}{d_{\text{reg}}}\right)^\omega$			$O(n \cdot \#Sol^3)$	

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

	Minors	Kipnis-Shamir
Degree of regularity when $n = (q - r)^2$	New $r(q - r) + 1$	New $d_{\text{reg}} \cdot (q - r)^2 + 2 < q(q - r) + 1$
# Sol		New $\prod_{i=0}^{q-r-1} \frac{i!(q+i)!}{(q-1-i)!(q-r+i)!}$
Complexity	$O(q^{3n})$	$O(q^{3(n+2)})$: polynomial in q

But... different **genericity assumptions** \rightsquigarrow bound not sharp

to be continued...



Courtois. Asiacrypt'01.

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

$\mathbb{K} = \mathbf{GF}(65521)$ (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	-
$\log_2(\text{Nb op.})$	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	7	
F_5 mem	407 MB	3113 MB	58587 MB		
$\log_2(\text{Nb op.})$	30.5	37.1	43.4		
FGLM time	35s	2580s	7		



Courtois. Asiacrypt'01.

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

$\mathbb{K} = \mathbf{GF}(65521)$ **(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	-
$\log_2(\text{Nb op.})$	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	7	
F_5 mem	407 MB	3113 MB	58587 MB		
$\log_2(\text{Nb op.})$	30.5	37.1	43.4		
FGLM time	35s	2580s	7		

Computational **bottleneck**: computing the minors.

Computing effort needed for solving **Challenge C**:

238 days on 64 quadricore processors.

Bilinear systems: particular case of **multi-homogeneous** systems

Multi-homogeneity

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

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

Bilinear systems: particular case of **multi-homogeneous** systems

Multi-homogeneity

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

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

- Real algebraic **geometry**

[Safey/Trébuchet 06, Bank/Giusti/Heintz/Safey/Schost AAECC'10].

Bilinear systems: particular case of **multi-homogeneous** systems

Multi-homogeneity

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

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

- Real algebraic **geometry**
[Safey/Trébuchet 06, Bank/Giusti/Heintz/Safey/Schost AAECC'10].

- \rightsquigarrow **Crypto**

1 Introduction

2 **MinRank**

1 Determinantal ideals

2 Multi-homogeneous systems

3 Applications in Cryptology

3 Quadratic boolean systems

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.

Modeling of McEliece cryptosystem

Based on **alternant codes**:

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

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

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 $H G^t = 0$!

Modeling of McEliece cryptosystem

Based on **alternant codes**:

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

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

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 , and H such that $H G^t = 0$!

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

) **Bi-homogeneous structure !!**

Compact variants

Goal: reduce the size of the keys.

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

Compact variants

Goal: reduce the size of the keys.

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

Faugère/Otmani/Perret/Tilich, Eurocrypt'2010

) 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**:

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

Compact variants

Goal: reduce the size of the keys.

- **Quasi-cyclic** variant: Berger/Cayrel/Gaborit/Otmani Africacrypt'09;
- **Dyadic** variant: Misoczky/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**:

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

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: Misoczky/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**:

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

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

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

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

Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt'96

Billet/Patarin/Seurin, ICSCC'08

Ding/Schmitt/Werner, Information Security, 2008

Granboulan/Joux/Stern, CRYPTO'06

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

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

Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt'96

Billet/Patarin/Seurin, ICSCC'08

Ding/Schmitt/Werner, Information Security, 2008

Granboulan/Joux/Stern, CRYPTO'06

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

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

Algebraic cryptanalysis of (multi-)HFE

Patarin, Eurocrypt'96

Billet/Patarin/Seurin, ICSCC'08

Ding/Schmitt/Werner, Information Security, 2008

Granboulan/Joux/Stern, CRYPTO'06

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

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

) the **secret polynomial** can be recovered by solving a **MinRank problem**.

Bettale/Faugère/Perret, PKC 2011

The **complexity** of solving this MinRank problem is conjectured to be bounded above by

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

↪ key-recovery attack with **polynomial complexity** in n !!

↪ attacks on **odd-characteristic** variants;

↪ generalizations to **multi-HFE**.

1 Introduction

2 MinRank

- Determinantal ideals
- Multi-homogeneous systems
- Applications in Cryptology

3 Quadratic boolean systems

Boolean systems (J. of Complexity 2012)

with M. Bardet, J.-C. Faugère, B. Salvy

Find **zeros** in \mathbb{F}_2^n of **quadratic polynomials** $f_1, \dots, f_m \in \mathbb{F}_2[x_1, \dots, x_n]$.

Find **zeros** in \mathbb{F}_2^n of **quadratic polynomials** $f_1, \dots, f_m \in \mathbb{F}_2[x_1, \dots, x_n]$.

State of the art:

- Worst case complexity $4 \cdot 2^n \log(n)$ (*Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10*).
- Exponentially better bounds conjectured (*Yang, Chen, Courtois*).

Boolean systems (*J. of Complexity 2012*)

with M. Bardet, J.-C. Faugère, B. Salvy

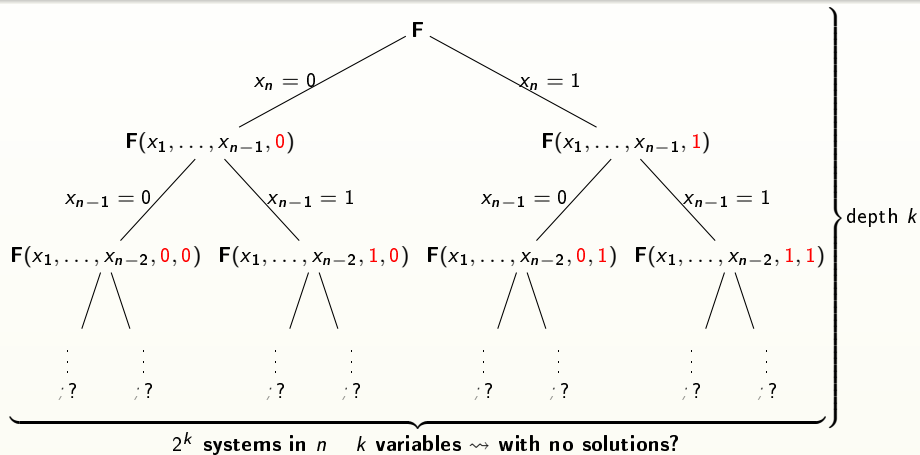
Find **zeros** in \mathbb{F}_2^n of **quadratic polynomials** $f_1, \dots, f_m \in \mathbb{F}_2[x_1, \dots, x_n]$.

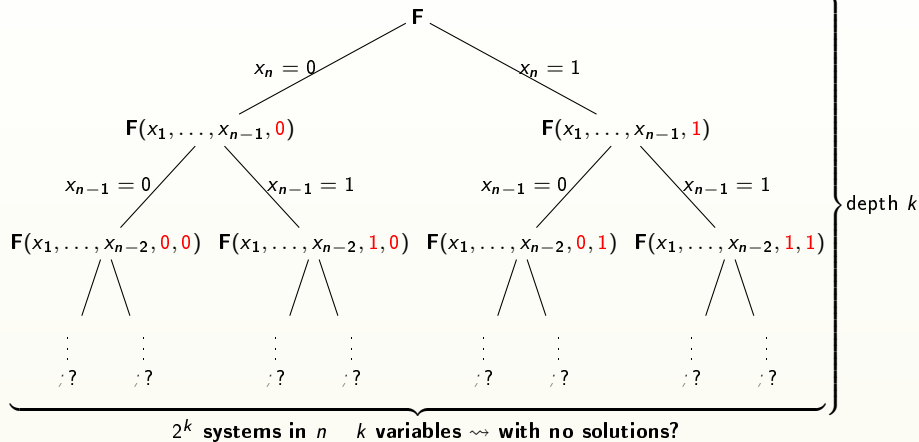
State of the art:

- Worst case complexity $4 \cdot 2^n \log(n)$ (*Bouillaguet, Chen, Cheng, Chou, Niederhagen, Yang, Shamir, CHES'10*).
- Exponentially better bounds conjectured (*Yang, Chen, Courtois*).

Main algorithmic result \rightsquigarrow **Algorithm:**

Exhaustive search + **sparse linear algebra** **pruning branches** in the search tree

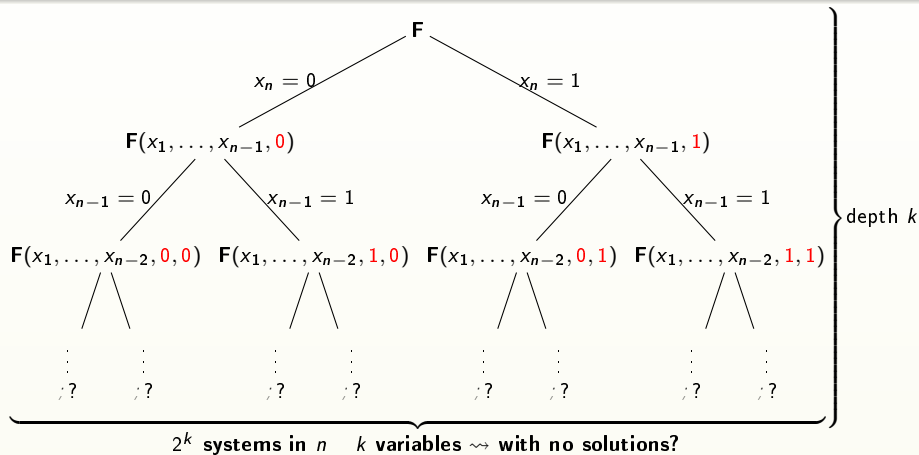




Hilbert Nullstellensatz

$F(x_1, \dots, x_{n-k}, a_{n-k+1}, \dots, a_n)$ has no solution in \mathbb{F}_2^{n-k}

$$1 \in \langle F, x_1^2, \dots, x_n^2 \rangle$$



Hilbert Nullstellensatz

$F(x_1, \dots, x_{n-k}, a_{n-k+1}, \dots, a_n)$ has no solution in \mathbb{F}_2^{n-k}
 $1 \in \langle F, x_1^2 - x_1, \dots, x_n^2 - x_n \rangle$

Can be tested by solving
a linear system
 involving the
Macaulay matrix

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \leq n > k$

f_1, \dots, f_m quadratic polynomials in $\mathbb{F}_2[x_1, \dots, x_n]$.

Output: The set of boolean solutions of the system $f_1 = \dots = f_m = 0$.

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \leq n > k$

f_1, \dots, f_m quadratic polynomials in $\mathbb{F}_2[x_1, \dots, x_n]$.

Output: The set of boolean solutions of the system $f_1 = \dots = f_m = 0$.

$S := \{ \}$.

$d_0 :=$ some integer.

(choice of a bound)

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \leq n > k$

f_1, \dots, f_m quadratic polynomials in $\mathbb{F}_2[x_1, \dots, x_n]$.

Output: The set of boolean solutions of the system $f_1 = \dots = f_m = 0$.

$S := \{ \}$.

$d_0 :=$ some integer.

(choice of a bound)

For all $(a_{n-k+1}, \dots, a_n) \in \mathbb{F}_2^k$

For i from 1 to m

(specialization)

$\tilde{f}_i(x_1, \dots, x_{n-k}) := f_i(x_1, \dots, x_{n-k}, a_{n-k+1}, \dots, a_n) \in \mathbb{F}_2[x_1, \dots, x_{n-k}]$.

EndFor

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \leq n > k$

f_1, \dots, f_m quadratic polynomials in $\mathbb{F}_2[x_1, \dots, x_n]$.

Output: The set of boolean solutions of the system $f_1 = \dots = f_m = 0$.

$S := \emptyset$.

$d_0 :=$ some integer.

(choice of a bound)

For all $(a_{n-k+1}, \dots, a_n) \in \mathbb{F}_2^k$

For i from 1 to m

(specialization)

$\tilde{f}_i(x_1, \dots, x_{n-k}) := f_i(x_1, \dots, x_{n-k}, a_{n-k+1}, \dots, a_n) \in \mathbb{F}_2[x_1, \dots, x_{n-k}]$.

EndFor

$M :=$ boolean Macaulay matrix of $(\tilde{f}_1, \dots, \tilde{f}_m)$ in degree d_0 .

If the system $\mathbf{u} \cdot M = (0 \ \dots \ 0 \ 1)$ is inconsistent

(pruning)

$T :=$ solutions of the system $(\tilde{f}_1 = \dots = \tilde{f}_m = 0)$ (exhaustive search).

For all $(t_1, \dots, t_{n-k}) \in T$

$S := S \cup \{f(t_1, \dots, t_{n-k}, a_{n-k+1}, \dots, a_n)\}$.

EndFor

EndIf

EndFor

Return S .

- 1 Choice of d_0 (in function of the number of specialized variables k)?
 \rightsquigarrow index of the **rst non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
 $\rightsquigarrow d_0 = M(\gamma)n$ when $k = (1 - \gamma)n$
- 2 Sizes of the Macaulay matrices (function of k)?
- 3 Complexity of the **consistency tests** (function of k)?
 $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
- 4 Find optimal k for **asymptotic complexity**?
 - Gauss: $k = 0.73n$;
 - Coppersmith-Winograd: $k = 0.60n$
 - Wiedemann: $k = 0.45n$.
- 5 **Degeneracy** phenomenoms?
 $\rightsquigarrow \gamma$ -strong semi-regularity.
- 6 Feasibility and applications?

- 1 Choice of d_0 (in function of the number of specialized variables k)?
 \rightsquigarrow index of the **rst non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
 $\rightsquigarrow d_0 = M(\gamma)n$ when $k = (1 - \gamma)n$
- 2 Sizes of the **Macaulay matrices** (function of k)?
- 3 Complexity of the **consistency tests** (function of k)?
 $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
- 4 Find optimal k for **asymptotic complexity**?
 - **Gauss**: $k = 0.73n$;
 - **Coppersmith-Winograd**: $k = 0.60n$
 - **Wiedemann**: $k = 0.45n$.
- 5 **Degeneracy** phenomenoms?
 $\rightsquigarrow \gamma$ -strong semi-regularity.
- 6 Feasibility and applications?

- 1 Choice of d_0 (in function of the number of specialized variables k)?
 \rightsquigarrow index of the **rst non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
 $\rightsquigarrow d_0 = M(\gamma)n$ when $k = (1 - \gamma)n$
- 2 Sizes of the **Macaulay matrices** (function of k)?
- 3 Complexity of the **consistency tests** (function of k)?
 $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
- 4 Find optimal k for **asymptotic complexity**?
 - **Gauss**: $k = 0.73n$;
 - **Coppersmith-Winograd**: $k = 0.60n$
 - **Wiedemann**: $k = 0.45n$.
- 5 **Degeneracy** phenomenoms?
 $\rightsquigarrow \gamma$ -strong semi-regularity.
- 6 Feasibility and applications?

1 Choice of d_0 (in function of the number of specialized variables k)?

\rightsquigarrow index of the **rst non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$

$\rightsquigarrow d_0 \approx M(\gamma)n$ when $k = (1 - \gamma)n$

2 Sizes of the **Macaulay matrices** (function of k)?

3 Complexity of the **consistency tests** (function of k)?

$O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$

4 Find optimal k for **asymptotic complexity**?

■ **Gauss**: $k = 0.73n$;

■ **Coppersmith-Winograd**: $k = 0.60n$

■ **Wiedemann**: $k = 0.45n$.

5 **Degeneracy** phenomenoms?

$\rightsquigarrow \gamma$ -strong semi-regularity.

6 Feasibility and applications?

- 1 Choice of d_0 (in function of the number of specialized variables k)?
 \rightsquigarrow index of the **rst non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
 $\rightsquigarrow d_0 = M(\gamma)n$ when $k = (1 - \gamma)n$
- 2 Sizes of the **Macaulay matrices** (function of k)?
- 3 Complexity of the **consistency tests** (function of k)?
 $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
- 4 Find optimal k for **asymptotic complexity**?
 - **Gauss**: $k = 0.73n$;
 - **Coppersmith-Winograd**: $k = 0.60n$
 - **Wiedemann**: $k = 0.45n$.
- 5 **Degeneracy** phenomenoms?
 $\rightsquigarrow \gamma$ -strong semi-regularity.
- 6 Feasibility and applications?

- 1 Choice of d_0 (in function of the number of specialized variables k)?
 \rightsquigarrow index of the **rst non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
 $\rightsquigarrow d_0 = M(\gamma)n$ when $k = (1 - \gamma)n$
- 2 Sizes of the **Macaulay matrices** (function of k)?
- 3 Complexity of the **consistency tests** (function of k)?
 $O(2^{(1-\gamma+\omega F(\gamma)+\varepsilon)n})$
- 4 Find optimal k for **asymptotic complexity**?
 - **Gauss**: $k = 0.73n$;
 - **Coppersmith-Winograd**: $k = 0.60n$
 - **Wiedemann**: $k = 0.45n$.
- 5 **Degeneracy** phenomenoms?
 $\rightsquigarrow \gamma$ -strong semi-regularity.
- 6 Feasibility and applications?

Linear solving – Wiedemann's algorithm

A linear system $A \mathbf{x} = \mathbf{b}$ can be solved within $\tilde{O}(\text{size}(A)^2)$ operations and $\tilde{O}(\text{size}(A))$ **evaluations** of the linear function $\mathbf{u} \nabla A \mathbf{u}$.

↔ exploits the **sparsity** of the **Macaulay matrix**
+ **Certificates** (Lobo/Giesbrecht/Saunders)

Complexity

Linear solving – Wiedemann's algorithm

A linear system $A \mathbf{x} = \mathbf{b}$ can be solved within $\tilde{O}(\text{size}(A)^2)$ operations and $\tilde{O}(\text{size}(A))$ **evaluations** of the linear function $\mathbf{u} \nabla A \mathbf{u}$.

↔ exploits the **sparsity** of the **Macaulay matrix**
+ **Certificates** (Lobo/Giesbrecht/Saunders)

Complexity analysis

Under precise *algebraic assumptions*, if $m = n$, the **complexity** is

- $O(2^{0.841n})$ with a **deterministic** variant;
- $O(2^{0.791n})$ with a **probabilistic** variant.

+ **generalizations** when $m = \alpha n$ ($\alpha < 1$).

Complexity

Linear solving – Wiedemann's algorithm

A linear system $A \mathbf{x} = \mathbf{b}$ can be solved within $\tilde{O}(\text{size}(A)^2)$ operations and $\tilde{O}(\text{size}(A))$ **evaluations** of the linear function $\mathbf{u} \nabla A \mathbf{u}$.

\rightsquigarrow exploits the **sparsity** of the **Macaulay matrix**
+ **Certificates** (Lobo/Giesbrecht/Saunders)

Complexity analysis

Under precise *algebraic assumptions*, if $m = n$, the **complexity** is

- $O(2^{0.841n})$ with a **deterministic** variant;
- $O(2^{0.791n})$ with a **probabilistic** variant.

+ **generalizations** when $m = \alpha n$ ($\alpha > 1$).

Experiments

- **Algebraic assumptions** are verified with **prob. close to 1**.
- Probabilistic variant: when $n = m$, **more efficient** than exhaustive search when $n \geq 200 \rightsquigarrow$ **Crypto applications** (QUAD).

Solving αn equations in n variables: $2^{c n}$

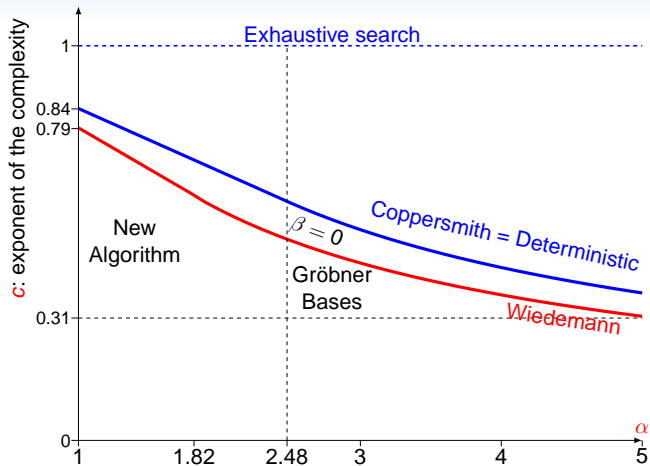


Figure: Exponent of the complexity in terms of α

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

Design techniques, keysize reduction, ... ! ^{Structure} potential algebraic **attacks**

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

Design techniques, key size reduction, ... ^{Structure} / potential algebraic attacks.

Algorithmic improvements

- Minrank Challenge (8, 9, 5)

[Crypto 2008] **328233s** → [Issac 2010] **935s** → [Pasco 2010] **73s**

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

Design techniques, key size reduction, ... ^{Structure} / potential algebraic attacks.

Algorithmic improvements

- Minrank Challenge (8, 9, 5)

[Crypto 2008] **328233s** → [Issac 2010] **935s** → [Pasco 2010] **73s**

Perspectives

- **Dedicated F_5 algorithm** for multi-homogeneous systems.
- Dedicated algorithm for **determinantal systems?**

Challenges

- **Systematic methodologies** for the analysis of **structures**

Challenges

- **Systematic methodologies** for the analysis of **structures** (Hilbert series, degree of regularity, tools for commutative algebra and algebraic geometry, invariants, ...).
- Impact of **ring isomorphisms** on Gröbner bases computations (\rightsquigarrow **multivariate Cryptography**).

Challenges

- **Systematic methodologies** for the analysis of **structures** (Hilbert series, degree of regularity, tools for commutative algebra and algebraic geometry, invariants, ...).
- Impact of **ring isomorphisms** on Gröbner bases computations (\rightsquigarrow **multivariate Cryptography**).
- **Algorithmic framework** for structured systems and implementation (representation of polynomials, parallelism, ...).

Challenges

- **Systematic methodologies** for the analysis of **structures** (Hilbert series, degree of regularity, tools for commutative algebra and algebraic geometry, invariants, ...).
- Impact of **ring isomorphisms** on Gröbner bases computations (\rightsquigarrow **multivariate Cryptography**).
- **Algorithmic framework** for structured systems and implementation (representation of polynomials, parallelism, ...).

Thank you!