Gröbner Bases of Structured Systems and Applications to Cryptology

Pierre-Jean Spaenlehauer

INRIA/CNRS/Univ. Lorraine, Caramel Project

Journées C2, March 26, 2014

Algebraic cryptanalysis

General framework

- Modeling of a **cryptosystem** by an algebraic **polynomial system**;
- Coefficients in a **finite field**;
- **Solving** $\longrightarrow$ retrieving secret information;
- **Complexity** $\longrightarrow$ security;
- Gröbner bases algorithms $\rightsquigarrow$ well-suited when $\mathbb{K}$ is a **finite field**.

Algebraic cryptanalysis

General framework

- Modeling of a **cryptosystem** by an algebraic **polynomial system**;
- Coefficients in a **finite field**;
- **Solving** $\rightarrow$ retrieving secret information;
- **Complexity** $\rightarrow$ security;
- Gröbner bases algorithms $\rightsquigarrow$ well-suited when $\mathbb{K}$ is a **finite field**.

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a finite field

$$\left\{ \begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{array} \right. \Longrightarrow$$

list the solutions in
$\mathbb{K}^n$
$\overline{\mathbb{K}}^n$

Algebraic cryptanalysis

General framework

- Modeling of a **cryptosystem** by an algebraic **polynomial system**;
- Coefficients in a **finite field**;
- **Solving** $\longrightarrow$ retrieving secret information;
- **Complexity** $\longrightarrow$ security;
- Gröbner bases algorithms $\rightsquigarrow$ well-suited when $\mathbb{K}$ is a **finite field**.

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a finite field

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{cases} \Longrightarrow \text{list the solutions in } \begin{matrix} \mathbb{K}^n \\ \overline{\mathbb{K}}^n \end{matrix}$$

NP-hard problem $\rightsquigarrow$ { **SAT** reduces to **PoSSo** when $\mathbb{K} = \mathbb{F}_2$; **Bézout theorem** $\rightsquigarrow$ d^n solutions in $\overline{\mathbb{K}}^n$. }

Algebraic cryptanalysis

General framework

- Modeling of a **cryptosystem** by an algebraic **polynomial system**;
- Coefficients in a **finite field**;
- **Solving** $\longrightarrow$ retrieving secret information;
- **Complexity** $\longrightarrow$ security;
- Gröbner bases algorithms $\rightsquigarrow$ well-suited when $\mathbb{K}$ is a **finite field**.

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a finite field

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{cases} \Longrightarrow$$

list the solutions in $\mathbb{K}^n$ / $\overline{\mathbb{K}}^n$

NP-hard problem $\rightsquigarrow$ $\begin{cases} \textbf{SAT} \text{ reduces to } \textbf{PoSSo} \text{ when } \mathbb{K} = \mathbb{F}_2 \\ \textbf{Bézout theorem} \rightsquigarrow d^n \text{ solutions in } \overline{\mathbb{K}}^n. \end{cases}$

But... **cryptographic properties** $\Longrightarrow$ **Structured** algebraic systems.

Algebraic cryptanalysis

General framework

- Modeling of a **cryptosystem** by an algebraic **polynomial system**;
- Coefficients in a **finite field**;
- **Solving** $\rightarrow$ retrieving secret information;
- **Complexity** $\rightarrow$ security;
- Gröbner bases algorithms $\rightsquigarrow$ well-suited when $\mathbb{K}$ is a **finite field**.

$f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a finite field

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{cases} \Longrightarrow$$

list the solutions in
$\mathbb{K}^n$
$\overline{\mathbb{K}}^n$

NP-hard problem $\rightsquigarrow$ { **SAT** reduces to **PoSSo** when $\mathbb{K} = \mathbb{F}_2$; **Bézout theorem** $\rightsquigarrow$ d^n solutions in $\overline{\mathbb{K}}^n$. }

But... **cryptographic properties** $\Longrightarrow$ **Structured** algebraic systems.

Question: impact of **structures** on **GB computations**.

0-dimensional solving strategy with Gröbner bases

$f_1 = \cdots = f_m = 0$		**Complexity**	**Algorithms**
$\Downarrow$ "grevlex" Gb	**Row Echelon** forms of Macaulay matrices up to degree $\mathsf{d}_{\mathsf{reg}}$	$O\left(m\binom{n+\mathsf{d}_{\mathsf{reg}}}{n}^{\omega}\right)$	**Buchberger (1965)** F_4 **(Faugère 1999)** F_5 **(Faugère 2002)**
$\Downarrow$ "lex" Gb	**Linear algebra** in $\frac{\mathbb{K}[\mathbf{X}]}{I}$ as a $\mathbb{K}$-vect. space of dim. $\mathrm{DEG}(I)$ $\rightsquigarrow g(u) = 0, x_i = h_i(u)$	$O\left(n\mathrm{DEG}(I)^3\right)$	**FGLM** Faugère, Gianni, Lazard, Mora (1993)

0-dimensional solving strategy with Gröbner bases

$f_1 = \cdots = f_m = 0$		**Complexity**	**Algorithms**
$\Downarrow$ "grevlex" Gb	**Row Echelon** forms of Macaulay matrices up to degree $\mathrm{d}_{\mathrm{reg}}$	$O\left(m\binom{n+\mathrm{d}_{\mathrm{reg}}}{n}^{\omega}\right)$	**Buchberger (1965)** **F_4 (Faugère 1999)** **F_5 (Faugère 2002)**
$\Downarrow$ "lex" Gb	**Linear algebra** in $\frac{\mathbb{K}[\mathbf{X}]}{I}$ as a $\mathbb{K}$-vect. space of dim. $\mathrm{DEG}(I)$ $\rightsquigarrow g(u) = 0, x_i = h_i(u)$	$O\left(n\mathrm{DEG}(I)^3\right)$	**FGLM** Faugère, Gianni, Lazard, Mora (1993)

Macaulay matrix in degree d

$f_1 = \cdots = f_m = 0, \deg(f_i) = d_i$
Rows: all products tf_i where $t \in \mathrm{Monomials}(d - d_i)$.
Columns: monomials of degree d.

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

0-dimensional solving strategy with Gröbner bases

		Complexity	Algorithms
$f_1 = \cdots = f_m = 0$ $\Downarrow$			
"grevlex" Gb	**Row Echelon** forms of Macaulay matrices up to degree d_{reg}	$O\left(m\binom{n+d_{reg}}{n}^{\omega}\right)$	**Buchberger (1965)** **F_4 (Faugère 1999)** **F_5 (Faugère 2002)**
$\Downarrow$ "lex" Gb	**Linear algebra** in $\frac{\mathbb{K}[\mathbf{X}]}{I}$ as a $\mathbb{K}$-vect. space of dim. $\mathrm{DEG}(I)$ $\rightsquigarrow g(u) = 0, x_i = h_i(u)$	$O\left(n\mathrm{DEG}(I)^3\right)$	**FGLM** Faugère, Gianni, Lazard, Mora (1993)

Macaulay matrix in degree d

$f_1 = \cdots = f_m = 0, \deg(f_i) = d_i$
Rows: all products tf_i where $t \in \mathrm{Monomials}(d - d_i)$.
Columns: monomials of degree d.

$$\begin{array}{c} \\ t_1 f_1 \\ \vdots \\ t_k f_m \end{array} \overset{m_1 > \cdots > m_\ell}{\left(\begin{array}{ccc} \quad & \quad & \quad \\ & & \\ & & \end{array}\right)}$$

Degree of regularity:
maximal degree reached

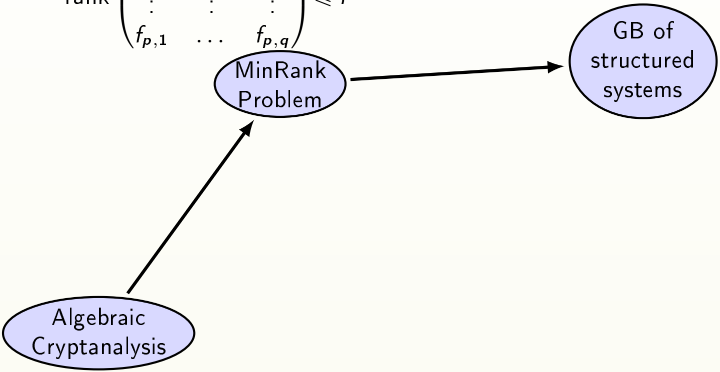
Hilbert series:
generating series of the rank defects

$$\mathrm{HS}(t) = \sum_{d \in \mathbb{N}} \dim(\mathbb{K}[X]_d / I_d) t^d$$

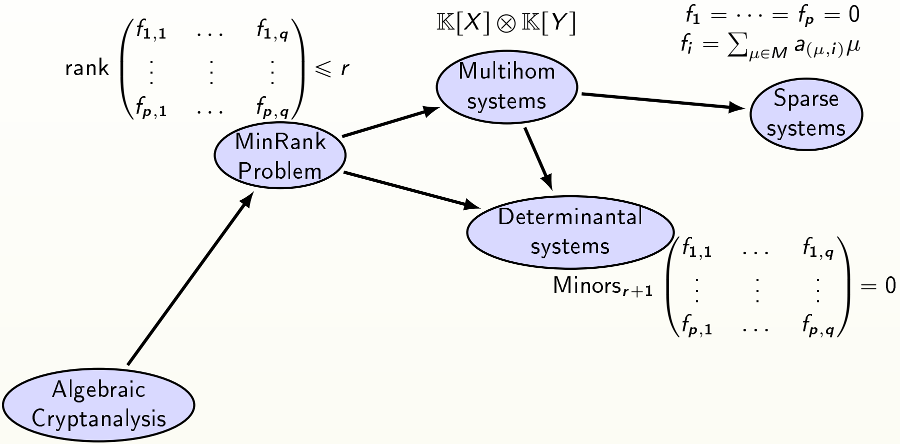
$$d_{reg} = \deg(\mathrm{HS}) + 1$$

Structured Systems in Cryptology

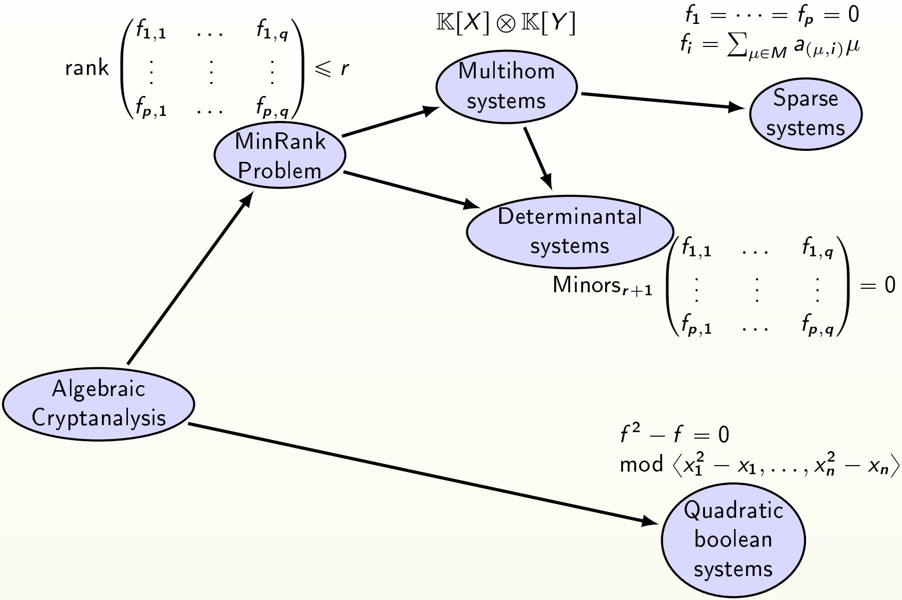
$$\operatorname{rank}\begin{pmatrix} f_{1,1} & \dots & f_{1,q} \\ \vdots & \vdots & \vdots \\ f_{p,1} & \dots & f_{p,q} \end{pmatrix} \leqslant r$$



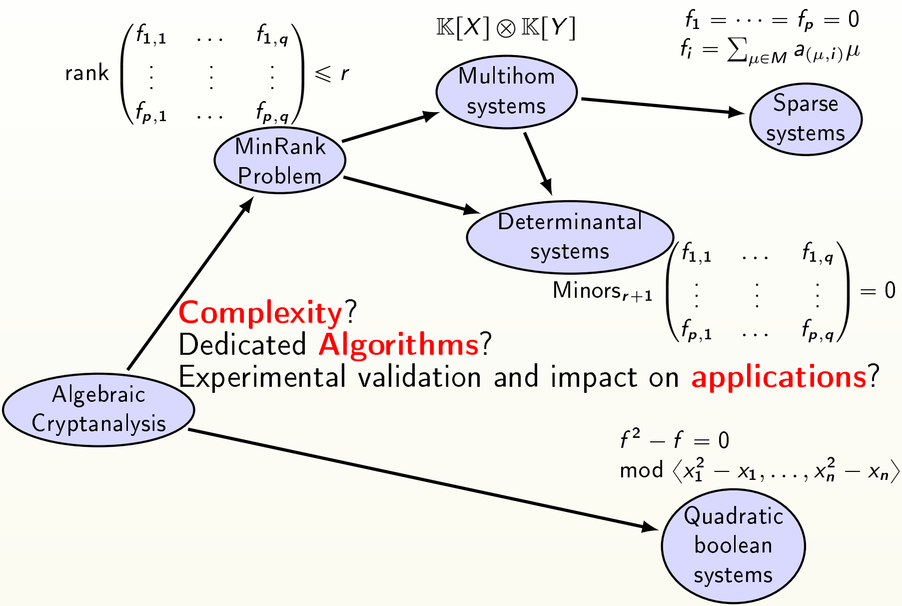
Structured Systems in Cryptology



Structured Systems in Cryptology

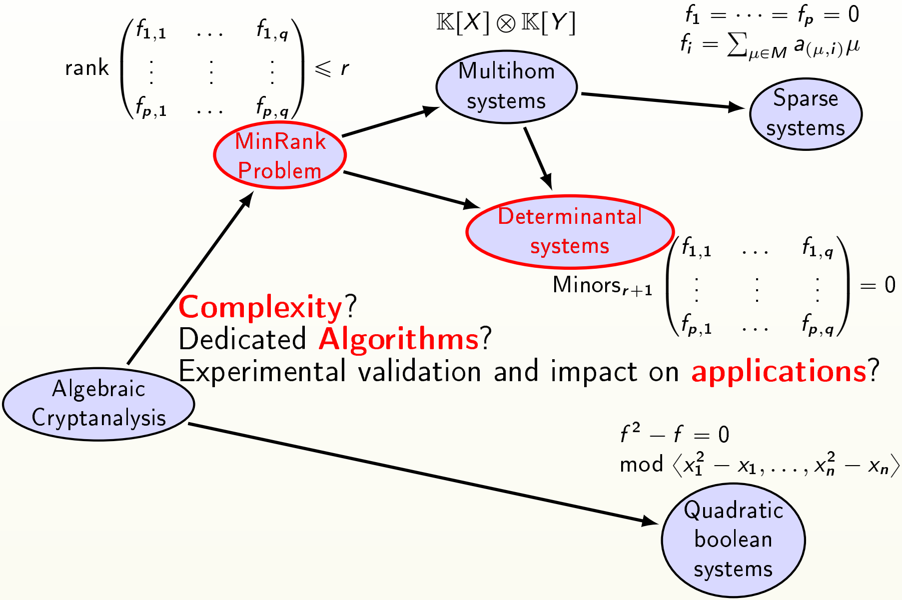


Structured Systems in Cryptology



Complexity?
Dedicated **Algorithms**?
Experimental validation and impact on **applications**?

Structured Systems in Cryptology



Complexity?
Dedicated **Algorithms**?
Experimental validation and impact on **applications**?

MinRank

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

MinRank Problem

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

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

MinRank

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

MinRank Problem

Find $\lambda_1, \ldots, \lambda_n$ such that

$$\textbf{Rank}\left(M_0 - \sum_{i=1}^{n} \lambda_i M_i\right) \leqslant r$$

- **Multivariate** generalization of the **EigenValue** problem.
- Applications in **cryptology**, **coding theory**, **geometry**, ...
  Kipnis/Shamir Crypto'99 Faugère/Levy-dit-Vehel/Perret, Crypto '08
  Courtois Crypto'01 Gaborit/Ruatta/Schrek'13
- Fundamental **NP-hard** problem of **linear algebra**.
  Buss/Frandsen/Shallit, 1999.

Determinantal systems

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

$$\mathrm{M}(X) = \begin{bmatrix} f_{1,1}(X) & \cdots & \cdots & f_{1,q}(X) \\ \vdots & \dots & \dots & \vdots \\ f_{p,1}(X) & \cdots & \cdots & f_{p,q}(X) \end{bmatrix}$$

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

Determinantal systems

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

$$\mathrm{M}(X) = \begin{bmatrix} f_{1,1}(X) & \cdots & \cdots & f_{1,q}(X) \\ \vdots & \dots & \dots & \vdots \\ f_{p,1}(X) & \cdots & \cdots & f_{p,q}(X) \end{bmatrix}$$

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

Generalized MinRank Problem

Compute the set of points $\mathbf{x} \in \overline{\mathbb{K}}^n$ such that $\mathrm{rank}(\mathrm{M}(\mathbf{x})) \leqslant r$.

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

Main results

with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D.
Zero-dimensional case ($n = (p-r)(q-r)$).

	System $\longrightarrow$ **grevlex GB**	$\underset{\text{Change of ordering}}{\longrightarrow}$ **lex GB**.
Complexity	$O\left(\left(\binom{\mathbf{p}}{\mathbf{r}+\mathbf{1}}\binom{\mathbf{q}}{\mathbf{r}+\mathbf{1}}\binom{\mathbf{n}+\mathbf{d}_{\mathbf{reg}}}{\mathbf{d}_{\mathbf{reg}}}\right)^{\omega}\right)$	$O\left(\mathbf{n}\cdot \mathrm{DEG}^3\right)$

Main results
with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D.
Zero-dimensional case ($n = (p-r)(q-r)$).

	System $\longrightarrow$ grevlex GB	$\xrightarrow{\text{Change of ordering}}$ lex GB.
Complexity	$O\left(\binom{\mathbf{p}}{\mathbf{r}+\mathbf{1}}\binom{\mathbf{q}}{\mathbf{r}+\mathbf{1}}\binom{\mathbf{n}+\mathbf{d}_{\mathrm{reg}}}{\mathbf{d}_{\mathrm{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot \mathrm{DEG}^3\right)$

Degree and regularity (under genericity assumptions on the coefficients)

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

Main results
with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D.
Zero-dimensional case ($n = (p-r)(q-r)$).

	System $\longrightarrow$ **grevlex GB**	$\underset{\text{Change of ordering}}{\longrightarrow}$ **lex GB**.
Complexity	$O\left(\binom{\mathbf{p}}{\mathbf{r+1}}\binom{\mathbf{q}}{\mathbf{r+1}}\binom{\mathbf{n+d_{reg}}}{\mathbf{d_{reg}}}^{\omega}\right)$	$O\left(\mathbf{n}\cdot \mathrm{DEG}^3\right)$

Degree and regularity (under genericity assumptions on the coefficients)

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

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

Main results
with J.-C. Faugère, M. Safey El Din

$p \times q$ matrix. n variables. Entries of degree D.
Zero-dimensional case ($n = (p-r)(q-r)$).

	System $\longrightarrow$ grevlex GB	$\overset{\longrightarrow}{\text{Change of ordering}}$ lex GB.
Complexity	$O\left(\binom{\mathbf{p}}{\mathbf{r}+\mathbf{1}}\binom{\mathbf{q}}{\mathbf{r}+\mathbf{1}}\binom{\mathbf{n}+\mathbf{d}_{\text{reg}}}{\mathbf{d}_{\text{reg}}}^{\omega}\right)$	$O\left(\mathbf{n} \cdot \text{DEG}^3\right)$

Degree and regularity (under genericity assumptions on the coefficients)

$$\mathrm{d}_{\text{reg}} = Dr(q-r) + (D-1)(p-r)(q-r) + 1$$

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

$\rightsquigarrow$ families of Generalized MinRank Problems that can be solved in complexity **polynomial** in the **number of solutions**.

Application in Cryptology

Courtois, Crypto'01
Authentication scheme based on the difficulty of MinRank. Proposed parameters:
$p = q$, $\mathbb{K} = \mathbb{F}_{65521}$, $r = q - 3$.

Application in Cryptology

Courtois, Crypto'01
Authentication scheme based on the difficulty of MinRank. Proposed parameters:
$p = q$, $\mathbb{K} = \mathbb{F}_{65521}$, $r = q - 3$.

Complexity of the algebraic attack: $O(q^9)$

Courtois, Crypto'01
Authentication scheme based on the difficulty of MinRank. Proposed parameters: $p = q$, $\mathbb{K} = \mathbb{F}_{65521}$, $r = q - 3$.

Complexity of the algebraic attack: $O(q^9)$

q	security	FGb F_5+FGLM
6	2^{106}	2.8s
7	2^{122}	130s
11	2^{138}	238 days (est.) on 64 quadcore proc.

Bottleneck for $q = 11$: computing the input system.

Roadmap of the proof

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

Entries are **variables**

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

Roadmap of the proof

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

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

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

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

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

Roadmap of the proof

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

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

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

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

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

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

Entries are **polynomials**

Roadmap of the proof

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

Thom/Porteous 71, Giambelli 04, Harris/Tu 84
The **degree** of $\mathscr{D}$ 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 $\mathscr{D}$ is

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

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

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

Entries are **polynomials**

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

Roadmap of the proof

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

Thom/Porteous 71, Giambelli 04, Harris/Tu 84
The **degree** of $\mathscr{D}$ 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 $\mathscr{D}$ is

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

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

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

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

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

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

Roadmap of the proof

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

Thom/Porteous 71, Giambelli 04, Harris/Tu 84
The **degree** of $\mathscr{D}$ 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 $\mathscr{D}$ is

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

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

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

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

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

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

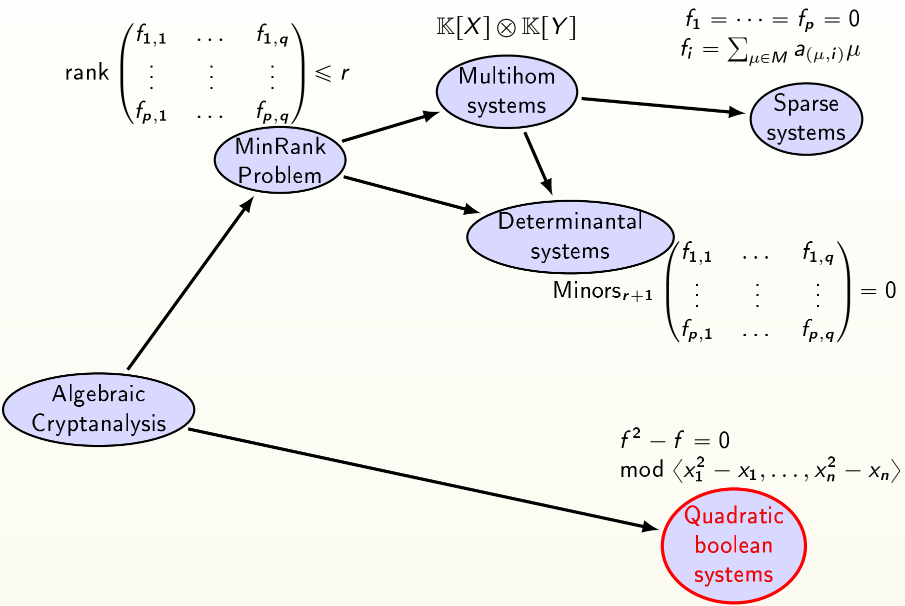
The **Hilbert series** of $\mathcal{I}$ is

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

Ingredients of the proof:

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

Structured Systems in Cryptology



Quadratic boolean systems
with M. Bardet, J.-C. Faugère, B. Salvy

Boolean MQ Problem

$f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ **quadratic polynomials.**
Find **one/all** **boolean solution** of the system

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & 0 \\ f_2(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{cases}$$

Quadratic boolean systems
with M. Bardet, J.-C. Faugère, B. Salvy

Boolean MQ Problem

$f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ **quadratic polynomials.**
Find **one/all** **boolean solution** of the system

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & 0 \\ f_2(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{cases}$$

- **NP-hard** problem $\rightsquigarrow$ SAT.
- Security of several modern **cryptosystems** relies on the difficulty of **Boolean MQ** (QUAD,...).
- Asymptotically, the number of solutions follows a **Poisson law** of parameter 2^{n-m} $\rightsquigarrow$ **few solutions** for **random** systems (*Fusco/Bach*, TAMC'07).
- Best proven **worst case complexity bound**: exhaustive search, $4 \cdot 2^n \log_2 n$ (*Bouillaguet/Chen/Cheng/Chou/Niederhagen/Shamir/Yang* CHES'10).

Quadratic boolean systems
with M. Bardet, J.-C. Faugère, B. Salvy

Boolean MQ Problem

$f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ **quadratic polynomials.**
Find **one/all** **boolean solution** of the system

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & 0 \\ f_2(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_m(x_1, \ldots, x_n) & = & 0 \end{cases}$$

- **NP-hard** problem $\rightsquigarrow$ SAT.
- Security of several modern **cryptosystems** relies on the difficulty of **Boolean MQ** (QUAD,...).
- Asymptotically, the number of solutions follows a **Poisson law** of parameter 2^{n-m} $\rightsquigarrow$ **few solutions** for **random** systems (*Fusco/Bach*, TAMC'07).
- Best proven **worst case complexity bound**: exhaustive search, $4 \cdot 2^n \log_2 n$ (*Bouillaguet/Chen/Cheng/Chou/Niederhagen/Shamir/Yang* CHES'10).

Problem: construct an $O(2^{cn})$ algorithm, with $\mathbf{c < 1}$.

Related works

Algorithmic Tools

- Exhaustive search: *Bouillaguet/Chen/Cheng/Chou/Niederhagen/Shamir/Yang* CHES'10,...;
- SAT-Solvers: *Davis/Putnam/Logemann/Loveland* J. of ACM'60, Comm. of ACM'62;
- Gröbner bases algorithms;
- Hybrid approach: *Bettale/Faugère/Perret* J. of Math. Crypto'09.

Related works

Algorithmic Tools

- Exhaustive search: *Bouillaguet/Chen/Cheng/Chou/Niederhagen/Shamir/Yang* CHES'10,. . . ;
- SAT-Solvers: *Davis/Putnam/Logemann/Loveland* J. of ACM'60, Comm. of ACM'62;
- Gröbner bases algorithms;
- Hybrid approach: *Bettale/Faugère/Perret* J. of Math. Crypto'09.

over $\mathbb{F}_2$, random systems $\neq$ generic systems

Main results

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

Algorithm:
use (sparse) **linear algebra** to prune useless subtrees in the exhaustive search tree.

Main results

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

Algorithm:
use (sparse) **linear algebra** to prune useless subtrees in the exhaustive search tree.

Complexity analysis

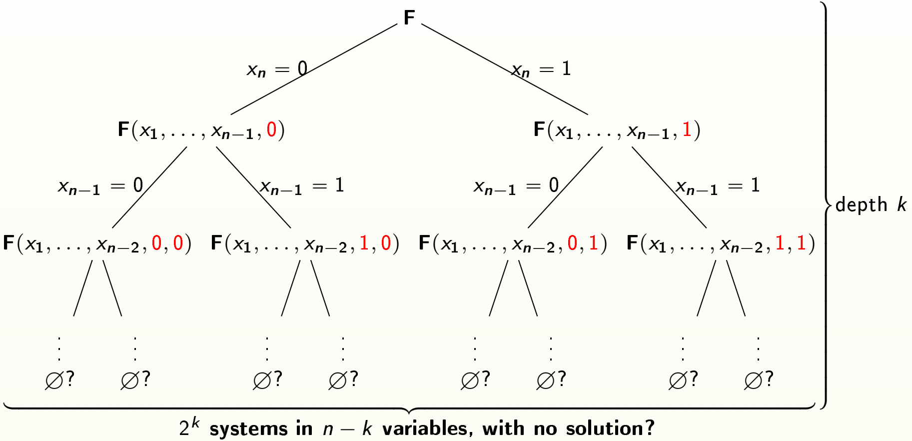
Under precise *algebraic assumptions*, if $m = n$, the **complexity** is

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

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

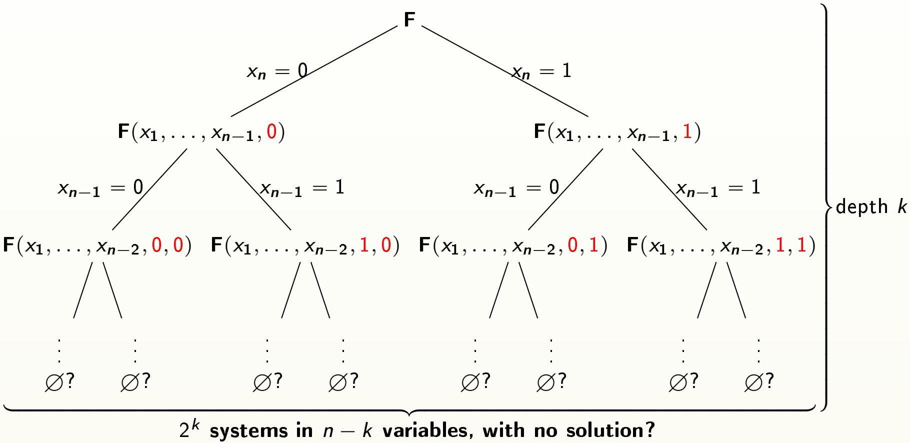
Algebraic assumptions: variant of **Fröberg Conjecture** on the algebraic structure of generic overdetermined systems.

Algorithm



F
$x_n = 0$
$x_n = 1$
$\mathbf{F}(x_1, \ldots, x_{n-1}, 0)$
$\mathbf{F}(x_1, \ldots, x_{n-1}, 1)$
$x_{n-1} = 0$
$x_{n-1} = 1$
$x_{n-1} = 0$
$x_{n-1} = 1$
$\mathbf{F}(x_1, \ldots, x_{n-2}, 0, 0)$
$\mathbf{F}(x_1, \ldots, x_{n-2}, 1, 0)$
$\mathbf{F}(x_1, \ldots, x_{n-2}, 0, 1)$
$\mathbf{F}(x_1, \ldots, x_{n-2}, 1, 1)$
$\varnothing$?
depth k
2^k **systems in** $n - k$ **variables, with no solution?**

Algorithm



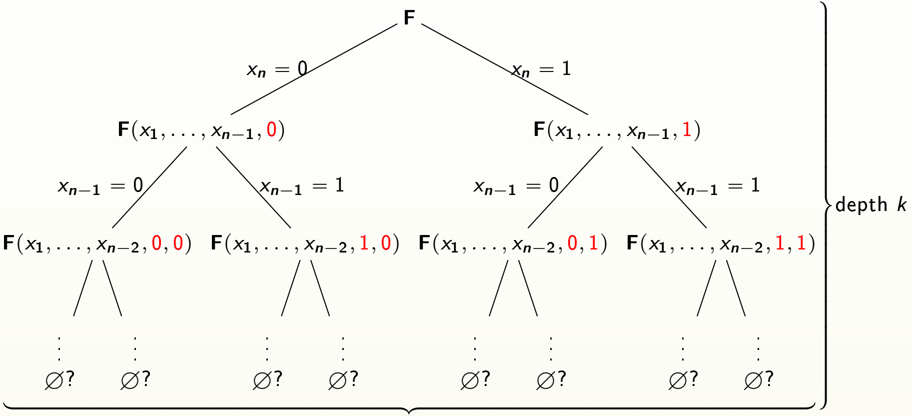
Hilbert Nullstellensatz

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

$$\Updownarrow$$

$$1 \in \langle \mathbf{F}, x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$$

Algorithm



2^k **systems in** $n-k$ **variables, with no solution?**

Hilbert Nullstellensatz

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

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

Boolean Macaulay matrix in degree d

$$I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{F}_2[x_1, \ldots, x_n].$$

Rows: all products tf_i where $t \in \text{SquareFreeMonomials}(d-2)$.
Columns: Square-free monomials of degree at most d.

$$\begin{array}{c} \\ t_1 f_1 \\ \vdots \\ t_k f_m \end{array} \begin{array}{c} m_1 > \cdots > m_\ell \\ \left(\begin{array}{ccc} & & \\ & & \\ & & \end{array} \right) \end{array} = \text{Mac}$$

Boolean Macaulay matrix in degree d

$$I = \langle f_1, \dots, f_m \rangle \subset \mathbb{F}_2[x_1, \dots, x_n].$$

Rows: all products tf_i where $t \in \text{SquareFreeMonomials}(d-2)$.
Columns: Square-free monomials of degree at most d.

$$\begin{array}{c} \\ t_1 f_1 \\ \vdots \\ t_k f_m \end{array} \quad \overset{m_1 \succ \cdots \succ m_\ell}{\left(\begin{array}{ccc} & & \\ & & \\ & & \end{array} \right)} = \text{Mac}$$

If the system has **no solution**, then $\exists g_1, \dots, g_m$, s.t.

$$\sum_{i=1}^{m} f_i g_i = 1 \mod \left\langle x_1^2 - x_1, \dots, x_n^2 - x_n \right\rangle \Rightarrow \exists v \text{ s.t. } v \cdot \text{Mac} = \begin{pmatrix} 0 & \dots & 0 & 1 \end{pmatrix}.$$

Boolean Macaulay matrix in degree d

$$I = \langle f_1, \dots, f_m \rangle \subset \mathbb{F}_2[x_1, \dots, x_n].$$

Rows: all products tf_i where $t \in \text{SquareFreeMonomials}(d-2)$.
Columns: Square-free monomials of degree at most d.

$$\begin{array}{c} \\ t_1 f_1 \\ \vdots \\ t_k f_m \end{array} \quad \begin{array}{c} m_1 \succ \cdots \succ m_\ell \\ \left(\begin{array}{c} \quad \\ \quad \\ \quad \end{array} \right) \end{array} = \text{Mac}$$

If the system has **no solution**, then $\exists g_1, \dots, g_m$, s.t.

$$\sum_{i=1}^{m} f_i g_i = 1 \mod \langle x_1^2 - x_1, \dots, x_n^2 - x_n \rangle \Rightarrow \exists v \text{ s.t. } v \cdot \text{Mac} = \begin{pmatrix} 0 & \dots & 0 & 1 \end{pmatrix}.$$

Deciding if the system has solutions or not is reduced to testing the consistency of a **sparse linear system**.

Boolean Macaulay matrix in degree d

$$I = \langle f_1, \dots, f_m \rangle \subset \mathbb{F}_2[x_1, \dots, x_n].$$

Rows: all products tf_i where $t \in \mathrm{SquareFreeMonomials}(d-2)$.
Columns: Square-free monomials of degree at most d.

$$\begin{array}{c} \\ t_1 f_1 \\ \vdots \\ t_k f_m \end{array} \quad \begin{array}{c} m_1 \succ \cdots \succ m_\ell \\ \left(\begin{array}{ccc} \quad & \quad & \quad \\ & & \\ & & \end{array} \right) \end{array} = \mathrm{Mac}$$

If the system has **no solution**, then $\exists g_1, \dots, g_m$, s.t.

$$\sum_{i=1}^{m} f_i g_i = 1 \mod \left\langle x_1^2 - x_1, \dots, x_n^2 - x_n \right\rangle \Rightarrow \exists v \text{ s.t. } v \cdot \mathrm{Mac} = \begin{pmatrix} 0 & \dots & 0 & 1 \end{pmatrix}.$$

Deciding if the system has solutions or not is reduced to testing the consistency of a **sparse linear system**.

Problem: which d?

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \geqslant n > k$
$f_1, \ldots, f_m$ quadratic polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$.
Output: The set of boolean solutions of the system $f_1 = \cdots = f_m = 0$.

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \geqslant n > k$
$f_1, \ldots, f_m$ quadratic polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$.
Output: The set of boolean solutions of the system $f_1 = \cdots = f_m = 0$.

$S := \varnothing$.
$d_0 :=$ some integer. **(choice of a bound)**

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \geqslant n > k$
$f_1, \dots, f_m$ quadratic polynomials in $\mathbb{F}_2[x_1, \dots, x_n]$.
Output: The set of boolean solutions of the system $f_1 = \cdots = f_m = 0$.

$S := \emptyset$.
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

Algorithm BooleanSolve

Input: $m, n, k \in \mathbb{N}$ such that $m \geqslant n > k$
$f_1, \ldots, f_m$ quadratic polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$.
Output: The set of boolean solutions of the system $f_1 = \cdots = f_m = 0$.

$S := \emptyset$.
$d_0 :=$ some integer. **(choice of a bound)**

For all $(a_{n-k+1}, \ldots, a_n) \in \mathbb{F}_2^k$
    For i from 1 to m **(specialization)**
        $\tilde{f}_i(x_1, \ldots, x_{n-k}) := f_i(x_1, \ldots, x_{n-k}, a_{n-k+1}, \ldots, a_n) \in \mathbb{F}_2[x_1, \ldots, x_{n-k}]$.
    EndFor
    M := **boolean Macaulay matrix** of $(\tilde{f}_1, \ldots, \tilde{f}_m)$ in degree d_0.
    If the system $\mathbf{u} \cdot \mathrm{M} = \begin{pmatrix} 0 & \ldots & 0 & 1 \end{pmatrix}$ is inconsistent **(pruning)**
        $T :=$ solutions of the system $(\tilde{f}_1 = \cdots = \tilde{f}_m = 0)$ (exhaustive search).
        For all $(t_1, \ldots, t_{n-k}) \in T$
            $S := S \cup \{(t_1, \ldots, t_{n-k}, a_{n-k+1}, \ldots, a_n)\}$.
        EndFor
    EndIf
EndFor
Return S.

Workplan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ 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?
   $\rightsquigarrow$ γ-strong semi-regularity.

Workplan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
   $$M(\gamma) = \left(-1/\gamma + 1/2 + 1/2\sqrt{2/\gamma^2 - 10/\gamma - 1 + 2(1/\gamma + 2)\sqrt{(1/\gamma + 2)/\gamma}}\right)\gamma.$$
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?
   $\rightsquigarrow$ γ-strong semi-regularity.

Workplan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\leadsto$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\leadsto$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
   $$M(\gamma) = \left(-1/\gamma + 1/2 + 1/2\sqrt{2/\gamma^2 - 10/\gamma - 1 + 2(1/\gamma + 2)\sqrt{(1/\gamma + 2)/\gamma}}\right)\gamma.$$
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?
   $\leadsto$ γ-strong semi-regularity.

Workplan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
   $$M(\gamma) = \left(-1/\gamma + 1/2 + 1/2\sqrt{2/\gamma^2 - 10/\gamma - 1 + 2(1/\gamma + 2)\sqrt{(1/\gamma+2)/\gamma}}\right)\gamma.$$
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?
   $\rightsquigarrow$ γ-strong semi-regularity.

Workplan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
   $$M(\gamma) = \left(-1/\gamma + 1/2 + 1/2\sqrt{2/\gamma^2 - 10/\gamma - 1 + 2(1/\gamma + 2)\sqrt{(1/\gamma + 2)/\gamma}}\right)\gamma.$$
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?
   $\rightsquigarrow$ γ-strong semi-regularity.

Workplan

1. Choice of d_0 (in function of the number of specialized variables k)?
   $\rightsquigarrow$ index of the **first non-positive coefficient** in $\frac{(1+t)^{n-k}}{(1-t)(1+t^2)^m}$
   $\rightsquigarrow$ $d_0 \sim M(\gamma)n$ when $k = (1-\gamma)n$
   $M(\gamma) = \left(-1/\gamma + 1/2 + 1/2\sqrt{2/\gamma^2 - 10/\gamma - 1 + 2(1/\gamma+2)\sqrt{(1/\gamma+2)/\gamma}}\right)\gamma.$
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?
   $\rightsquigarrow$ γ-strong semi-regularity.

Complexity

Complexity analysis

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

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

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

Complexity

Complexity analysis

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

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

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

Experiments

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

Variant of Fröberg conjecture

The **proportion** of γ-strong semi-regular systems tends to 1 when $n \to \infty$.

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

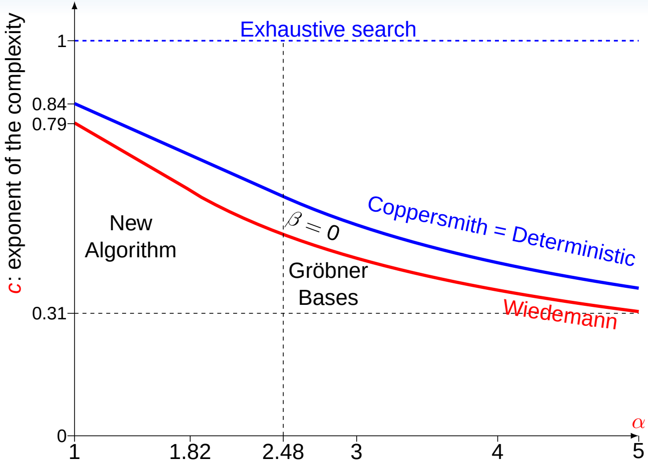


Figure: Exponent of the complexity in terms of α

Conclusion and Perspectives

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

Conclusion and Perspectives

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

Algorithmic improvements

- Minrank Challenge $(8, 9, 5)$
  [Crypto 2008] **328233s** ⟶ [Issac 2010] **935s** ⟶ [Pasco 2010] **73s**
  Faugère/Levy-dit-Vehel/Perret — Faugère/S./Safey — Faugère/Lachartre
- Dedicated F_5 algorithm for multi-homogeneous/sparse systems (speed-up more than 100 for some overdetermined bihomogeneous systems)
  $\rightsquigarrow$ *Faugère/S./Svartz*, arXiv:1402.7205, 2014

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

Algorithmic improvements

- Minrank Challenge $(8, 9, 5)$
  [Crypto 2008] **328233s** $\longrightarrow$ [Issac 2010] **935s** $\longrightarrow$ [Pasco 2010] **73s**
  Faugère/Levy-dit-Vehel/Perret — Faugère/S./Safey — Faugère/Lachartre
- Dedicated F_5 algorithm for multi-homogeneous/sparse systems (speed-up more than 100 for some overdetermined bihomogeneous systems)
  $\rightsquigarrow$ *Faugère/S./Svartz*, arXiv:1402.7205, 2014

Perspectives

- Dedicated algorithm for **determinantal systems**?

Long term perspectives

Challenges

- **Systematic methodologies** for the analysis of **structures** (Hilbert series, degree of regularity, tools for commutative algebra and algebraic geometry, invariants,. . .).

Long term perspectives

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**).

Long term perspectives

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!