Gröbner bases techniques in Cryptography

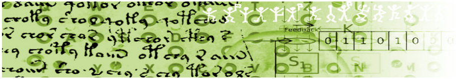
Ludovic Perret

SALSA
LIP6, Université Paris 6 & INRIA Paris-Rocquencourt
ludovic.perret@lip6.fr

Plan

1. Algebraic Cryptanalysis
2. MinRank
3. Solving MinRank (Faugère/Levy/Perret, CRYPTO'08)
   - Kipnis-Shamir
   - Experimental Results
   - Theoretical Analysis (Faugère, Safey El Din, Spaenlehauer, ISSAC'10).

General Context



C.E. Shannon

Communication Theory of Secrecy Systems (1949)

"Breaking a good cipher should require as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type."

Algebraic Cryptanalysis

Principle

- Model a cryptosystem as a set of **non-linear equations**
- Try to **solve** this system (or **estimate** the difficulty of solving)

Approach

Difficulties

- Model a cryptosystem as a set of **non-linear equations**
  - “universal" approach (PoSSo is NP-Hard)
    - $\Rightarrow$ several models are possible !!!
- Solving
  - $\Rightarrow$ Minimize the number of variables/degree
  - $\Rightarrow$ Maximize the number of equations

Approach

Difficulties

- Model a cryptosystem as a set of **non-linear equations**

  "universal" approach (PoSSo is NP-Hard)

  $\Rightarrow$ several models are possible !!!
- Solving

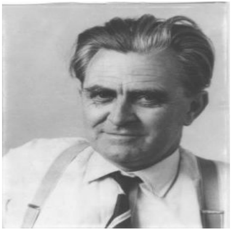
  $\Rightarrow$ Minimize the number of variables/degree

  $\Rightarrow$ Maximize the number of equations

Specificity

Solving algebraic systems :

- Gröbner bases



Gröbner Basis

$\mathbb{K}$: **finite field** $\mathbb{K}[x_1, \ldots, x_n]$: **polynomial ring** in n variables**.**

Linear Systems

$$\begin{cases} x_1 + x_2 - 1 = 0 \\ x_1 - x_2 = 0 \end{cases}$$

Gröbner Basis

$\mathbb{K}$: **finite field** $\quad$ $\mathbb{K}[x_1, \ldots, x_n]$: **polynomial ring** in n variables.

Linear Systems

$$\begin{cases} x_1 + x_2 - 1 = 0 \\ x_1 - x_2 = 0 \end{cases}$$

Polynomial Systems

$$\begin{cases} x_1 x_2 - x_2^2 = 0, \\ x_1^2 - x_1 = 0 \end{cases}$$

Gröbner Basis

$\mathbb{K}$: **finite field** $\mathbb{K}[x_1, \ldots, x_n]$: **polynomial ring** in n variables.

Linear Systems

$$\begin{cases} \ell_1(x_1, \ldots, x_n) = 0 \\ \ell_2(x_1, \ldots, x_n) = 0 \\ \vdots \\ \ell_m(x_1, \ldots, x_n) = 0 \end{cases}$$

Polynomial Systems

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

Gröbner Basis

$\mathbb{K}$: **finite field** $\quad \mathbb{K}[x_1, \ldots, x_n]$: **polynomial ring** in n variables.

Linear Systems

$$\begin{cases} \ell_1(x_1, \ldots, x_n) = 0 \\ \ell_2(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ \ell_m(x_1, \ldots, x_n) = 0 \end{cases}$$

- $V = \mathrm{Vect}_{\mathbb{K}}(\ell_1, \ldots, \ell_m)$
- **Triangular/diagonal basis** of V

Polynomial Systems

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

Gröbner Basis

$\mathbb{K}$: **finite field** $\quad \mathbb{K}[x_1, \ldots, x_n]$: **polynomial ring** in n variables.

Linear Systems

$$\begin{cases} \ell_1(x_1, \ldots, x_n) = 0 \\ \ell_2(x_1, \ldots, x_n) = 0 \\ \quad\vdots \\ \ell_m(x_1, \ldots, x_n) = 0 \end{cases}$$

- $V = \mathrm{Vect}_{\mathbb{K}}(\ell_1, \ldots, \ell_m)$
- **Triangular/diagonal basis** of V

Polynomial Systems

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

- **Ideal** $\mathcal{I} = \langle f_1, \ldots, f_m \rangle =$

$$\left\{ \sum_{i=1}^{m} f_i u_i \mid u_i \in \mathbb{K}[x_1, \ldots, x_n] \right\}.$$

- Gröbner basis of $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$

Gröbner Basis

- Fix an ordering on the **monomials** (i.e. a power product $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$) of $\mathbb{K}[x_1, \ldots, x_n]$.

Lexicographical

$x_1 >_{\mathrm{Lex}} x_2 >_{\mathrm{Lex}} \cdots >_{\mathrm{Lex}} x_n$.

$$x_1 x_2 >_{\mathrm{Lex}} x_1 x_2^2$$

Gröbner Basis

- Fix an ordering on the **monomials** (i.e. a power product $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$) of $\mathbb{K}[x_1, \ldots, x_n]$.

Lexicographical

$x_1 >_{\mathrm{Lex}} x_2 >_{\mathrm{Lex}} \cdots >_{\mathrm{Lex}} x_n$.

$$x_1 x_2 >_{\mathrm{Lex}} x_1 x_2^2$$

DRL (Degree ordering)

$$x_1 x_2 <_{\mathrm{DRL}} x_1 x_2^2.$$

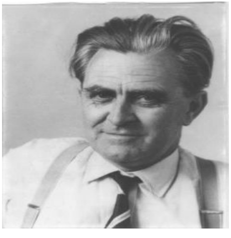
Gröbner Basis

- Fix an ordering on the **monomials** (i.e. a power product $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$) of $\mathbb{K}[x_1, \ldots, x_n]$.

Definition (Buchberger 1965/1976)

Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. A subset $G \subset \mathcal{I}$ is a Gröbner basis if:

$$\forall f \in \mathcal{I}, \exists g \in G \text{ s. t. } \mathrm{LM}(g) \text{ divides } \mathrm{LM}(f).$$

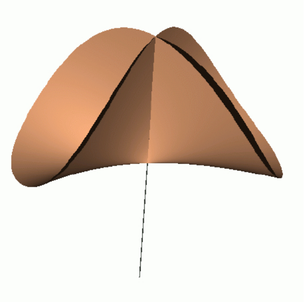


LEX Gröbner Basis

Problem

- $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$
- Compute $V_{\mathbb{K}}(f_1, \ldots, f_m) =$

$$\left\{ \mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{K}^n \mid f_1(\mathbf{z}) = 0, \ldots, f_m(\mathbf{z}) = 0 \right\}$$



LEX Gröbner Basis

Problem

- $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n) \in \mathbb{K}[x_1,\ldots,x_n]$
- Compute $V_{\mathbb{K}}(f_1,\ldots,f_m) =$

$$\left\{\mathbf{z} = (z_1,\ldots,z_n) \in \mathbb{K}^n \mid f_1(\mathbf{z}) = 0,\ldots,f_m(\mathbf{z}) = 0\right\}$$

Lemma

Let $\mathcal{I} = \langle f_1,\ldots,f_m, x_1^p - x_1,\ldots,x_n^p - x_n\rangle$, with $p = Char(\mathbb{K})$. A LEX Gröbner basis of a zero-dimensional system is always as follows :

$$\{g_1(x_1), g_2(x_1,x_2),\ldots,g_{k_2}(x_1,x_2), g_{k_2+1}(x_1,x_2,x_3),\ldots,\ldots\}$$

Change of ordering

Computing LEX is much more slower than computing DRL

J.-C. Faugère , P. Gianni, D. Lazard, and T. Mora.
Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering.
J. Symb. Comp., 1993.

Fact

D : the nb. of zeroes (with multiplicities) of $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$.
FGLM computes a DRL-Gröbner basis of $\mathcal{I}$ knowing a LEX Gröbner basis in :

$$\mathcal{O}(nD^3).$$

Zero-Dim Solving : a Two Steps Process

- Compute a Gröbner basis w.r.t DRL

  “computationally easy order"

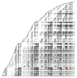
  - Buchberger’s algorithm (1965)
  - F_4/F_5 (J.-C. Faugère, 1999/2002)

  ⇒ For a zero-dimensional (i.e. finite number of solutions) system of *n* variables:

$$\mathcal{O}\left(n^{3 \cdot d_{reg}}\right),$$

  d_{reg} being the **maximum degree** reached during the computation.

Zero-Dim Solving : a Two Steps Process



- Compute a Gröbner basis w.r.t DRL

  “computationally easy order"

  - Buchberger’s algorithm (1965)
  - F_4/F_5 (J.-C. Faugère, 1999/2002)

  ⇒ For a zero-dimensional (i.e. finite number of solutions) system of n variables:

$$\mathcal{O}\left(n^{3\cdot d_{reg}}\right),$$

  d_{reg} being the **maximum degree** reached during the computation.

Zero-Dim Solving : a Two Steps Process

- Compute a Gröbner basis w.r.t DRL

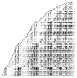
  "computationally easy order"

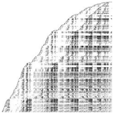
  - Buchberger's algorithm (1965)
  - F_4/F_5 (J.-C. Faugère, 1999/2002)

  $\Rightarrow$ For a zero-dimensional (i.e. finite number of solutions) system of n variables:

$$\mathcal{O}\left(n^{3 \cdot d_{reg}}\right),$$

d_{reg} being the **maximum degree** reached during the computation.





Zero-Dim Solving : a Two Steps Process

- Compute a Gröbner basis w.r.t DRL

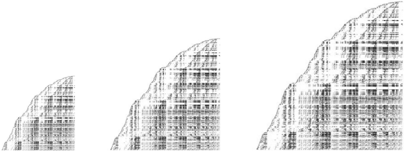
  “computationally easy order"

  - Buchberger’s algorithm (1965)
  - F_4/F_5 (J.-C. Faugère, 1999/2002)

  ⇒ For a zero-dimensional (i.e. finite number of solutions) system of n variables:

$$\mathcal{O}\left(n^{3 \cdot d_{reg}}\right),$$

d_{reg} being the **maximum degree** reached during the computation.



Zero-Dim Solving : a Two Steps Process

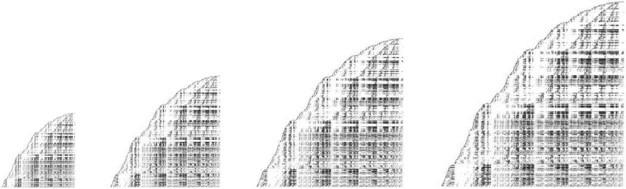
- Compute a Gröbner basis w.r.t DRL

  “computationally easy order"
  - Buchberger’s algorithm (1965)
  - F_4/F_5 (J.-C. Faugère, 1999/2002)

  $\Rightarrow$ For a zero-dimensional (i.e. finite number of solutions) system of n variables:

$$\mathcal{O}\left(n^{3\cdot d_{reg}}\right),$$

d_{reg} being the **maximum degree** reached during the computation.



Zero-Dim Solving : a Two Steps Process

- Compute a Gröbner basis w.r.t DRL

  “computationally easy order"
  - Buchberger’s algorithm (1965)
  - F_4/F_5 (J.-C. Faugère, 1999/2002)

  $\Rightarrow$ For a zero-dimensional (i.e. finite number of solutions) system of n variables:

  $$\mathcal{O}\left(n^{3\cdot d_{reg}}\right),$$

  d_{reg} being the maximum degree reached during the computation.

- If $\#$eq.$=\#$var :
  - d_{reg} is gen. equal to $n+1$.
  - $\#\mathcal{S}ol \leq \prod_{i=1}^{n} \mathrm{degreeEq}_i$ (**Bezout’s bound**)

Random Cases

For a *semi-regular* system of $m\,(> n)$ quadratic equations over $\mathbb{K}[x_1, \ldots, x_n]$ the degree of regularity is obtained from:

$$\sum_{i \geq 0} a_i z^i = \frac{(1 - z^2)^m}{(1 - z)^n}.$$

Random Cases

For a *semi-regular* system of $m\,(> n)$ quadratic equations over $\mathbb{K}[x_1, \ldots, x_n]$ the degree of regularity is obtained from:

$$\sum_{i \geq 0} a_i z^i = \frac{(1-z^2)^m}{(1-z)^n}.$$

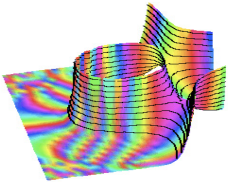
Example (3 variables and 5 equations)

$$1 + 3 \cdot x + x^2 - 5 \cdot x^3 - 5 \cdot x^4 + x^5 + 3 \cdot x^6 + x^7 + \cdots$$

Random Cases

For a *semi-regular* system of $m\,(> n)$ quadratic equations over $\mathbb{K}[x_1, \ldots, x_n]$ the degree of regularity is obtained from:

$$\sum_{i \geq 0} a_i z^i = \frac{(1 - z^2)^m}{(1 - z)^n}.$$



M. Bardet, J-C. Faugère, B. Salvy and B-Y. Yang.
Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems.
MEGA 2005.

- If $m = n + 1$, $d_{reg} \sim_{n \to \infty} \left\lceil \frac{(n+1)}{2} \right\rceil$.

Random Cases

For a *semi-regular* system of $m\,(> n)$ quadratic equations over $\mathbb{K}[x_1,\ldots,x_n]$ the degree of regularity is obtained from:

$$\sum_{i\geq 0} a_i z^i = \frac{(1-z^2)^m}{(1-z)^n}.$$

- If $m = n+1$:

$$d_{reg} = \left\lceil \frac{(n+1)}{2} \right\rceil.$$

A. Szanto.
Multivariate Subresultants using Jouanolou's Resultant Matrices.
Journal of Pure and Applied Algebra.

Plan

1. Algebraic Cryptanalysis
2. MinRank
3. Solving MinRank (Faugère/Levy/Perret, CRYPTO'08)
   - Kipnis-Shamir
   - Experimental Results
   - Theoretical Analysis (Faugère, Safey El Din, Spaenlehauer, ISSAC'10).

The MinRank problem

J.O. Shallit, G.S. Frandsen, and J.F. Buss. *"The Computational Complexity of some Problems of Linear Algebra".* BRICS series report, 1996.

MR_0

Input: R a commutative ring, $n, k \in \mathbb{N}^{\cdot}$, $M \in \mathcal{M}_{n \times n}(R \cup \{x_1, \ldots, x_k\})$, and a target rank $r \in \mathbb{N}^{\cdot}$.
Question: decide if there exists $(\lambda_1, \ldots, \lambda_k) \in R^k$ such that:

$$\mathrm{Rank}\big(M(\lambda_1, \ldots, \lambda_k)\big) \leq r.$$

Theorem (SFB'96)

MR_0 is NP-Complete if R is a finite field.

The MinRank problem

N. Courtois.
"Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank". ASIACRYPT 2001.

MinRank (MR)

Input: $n, m, k \in \mathbb{N}^{\cdot}, M_0, \ldots, M_k \in \mathcal{M}_{n \times m}(\mathbb{K})$, and $r \in \mathbb{N}^{\cdot}$.
Question: decide if there exists $(\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$ such that:

$$\mathrm{Rank}\left(\sum_{j=1}^{k} \lambda_j M_j - M_0\right) \leq r.$$

Theorem (Courtois'2001)

MR *is NP-Complete.*

The MinRank problem

N. Courtois.
"Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank". ASIACRYPT 2001.

MinRank (MR)

Input: $n, m, k \in \mathbb{N}^{\cdot}, M_1, \ldots, M_k \in \mathcal{M}_{n \times m}(\mathbb{K})$, and $r \in \mathbb{N}^{\cdot}$.
Question: decide if there exists $(\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$ such that:

$$\mathrm{Rank}\left(\sum_{j=1}^{k} \lambda_j M_j\right) = r.$$

Theorem (Courtois'2001)

MR *is NP-Complete.*

Applications of MinRank

- **Rank Decoding**
  - A. V. Ourivski, T. Johansson.
    “New technique for decoding codes in the rank metric and its cryptography applications." Problems of Info. Transmission’2002
- **Matrix Rigidity**
  - A. Kumar, S. V. Lokam, Vi. M. Patankar, J. Sarma.
    “Using Elimination Theory to construct Rigid Matrices". FSTTCS’09.

Applications of MinRank

- **Zero-Knowledge authentication protocol** based on MR

  N. Courtois.
  "Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank". ASIACRYPT 2001.

- **Key Recovery** on Multivariate Public Key Cryptosystems

  A. Kipnis, A. Shamir.
  "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization". CRYPTO 99.

  N. Courtois, L. Goubin.
  "Cryptanalysis of the TTM Cryptosystem". ASIACRYPT 2000.

  L. Bettale, J.-C. Faugère, L. Perret.
  "Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants". PKC 2011

Outline

1. Algebraic Cryptanalysis
2. MinRank
3. Solving MinRank (Faugère/Levy/Perret, CRYPTO'08)
   - Kipnis-Shamir
   - Experimental Results
   - Theoretical Analysis (Faugère, Safey El Din, Spaenlehauer, ISSAC'10).

Kipnis-Shamir's Modeling – (I)

A. Kipnis and A. Shamir.
"Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization". CRYPTO 99.

Given $n, k \in \mathbb{N}^{\cdot}$; $M_1, \ldots, M_k \in \mathcal{M}_{n\times n}(\mathbb{K})$, and $r \in \mathbb{N}^{\cdot}$.

- Find $\lambda = (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$ such that:

$$\mathrm{Rk}\left(\sum_{j=1}^{k} \lambda_j M_j\right) = r.$$

Kipnis-Shamir's Modeling – (I)

A. Kipnis and A. Shamir.
"Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization". CRYPTO 99.

Given $n, k \in \mathbb{N}^{\cdot}$; $M_1, \ldots, M_k \in \mathcal{M}_{n\times n}(\mathbb{K})$, and $r \in \mathbb{N}^{\cdot}$.

- Find $\lambda = (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$ such that:

$$\mathrm{Rk}\left(\sum_{j=1}^{k} \lambda_j M_j\right) = r.$$

- Set $E_\lambda = \sum_{j=1}^{k} \lambda_j M_j$:

$\mathrm{Rk}(E_\lambda) = r \Leftrightarrow \exists (n-r)$ **linearly indep. vectors** $X^{(i)} \in \mathrm{Ker}(E_\lambda)$.

Kipnis-Shamir's Modeling – (I)

A. Kipnis and A. Shamir.
"Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization". CRYPTO 99.

Given $n, k \in \mathbb{N}^{\cdot}$; $M_1, \ldots, M_k \in \mathcal{M}_{n \times n}(\mathbb{K})$, and $r \in \mathbb{N}^{\cdot}$.

- Find $\lambda = (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$ such that:

$$\mathrm{Rk}\left(\sum_{j=1}^{k} \lambda_j M_j\right) = r.$$

- Set $E_\lambda = \sum_{j=1}^{k} \lambda_j M_j$:

  $\mathrm{Rk}(E_\lambda) = r \Leftrightarrow \exists (n-r)$ **linearly indep. vectors** $X^{(i)} \in \mathrm{Ker}(E_\lambda)$.

- We have $\left(\sum_{j=1}^{k} \lambda_j M_j\right) X^{(i)} = \mathbf{0}_n$, for all i, $1 \leq i \leq n-r$.

Kipnis-Shamir's Modeling – (II)

- Set $E_\lambda = \sum_{j=1}^{k} \lambda_j M_j$:

  $\mathrm{Rk}(E_\lambda) = r \Leftrightarrow \exists (n-r)$ **linearly indep. vectors** $X^{(i)} \in \mathrm{Ker}(E_\lambda)$.

- Let $X^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)})$, where $x_j^{(i)}$s are variables. Then :

$$\left(\sum_{j=1}^{k} y_j M_j\right) \begin{pmatrix} x_1^{(1)} & \cdots & x_1^{(n-r)} \\ x_2^{(1)} & \cdots & x_2^{(n-r)} \\ \vdots & \vdots & \vdots \\ x_n^{(1)} & \cdots & x_n^{(n-r)} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

Kipnis-Shamir's Modeling – (III)

- $\boxed{\text{Write } X^{(i)} = (e_i, x_1^{(i)}, \ldots, x_r^{(i)})}$, where $e_i \in \mathbb{K}^{n-r}$ and $x_j^{(i)}$s are variables:

$$\left(\sum_{j=1}^{k} y_j M_j\right) \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \\ x_1^{(1)} & \cdots & \cdots & x_1^{(n-r)} \\ \vdots & \vdots & \vdots & \vdots \\ x_r^{(1)} & \cdots & \cdots & x_r^{(n-r)} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

- $\mathcal{I}_{\mathrm{KS}}$: ideal generated by these $(n-r)n$ quadratic equations with $r(n-r)+k$ variables over $\mathbb{K}$.

Courtois' Authentication Scheme – Challenges

N. Courtois.
"Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank". ASIACRYPT 2001.

$\mathbb{F}_{65521}$

A: $n = 6, k = 10, r = 3$

- 18 eq., 19 var.

B: $n = 7, k = 10, r = 4$

- 21 eq., 22 variables

C: $n = 11, k = 10, r = 8$

- 33 eq., 35 variables

Courtois' Authentication Scheme – Challenges

N. Courtois.
"Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank". ASIACRYPT 2001.

$\mathbb{F}_{65521}$

A: $n = 6, k = 10, r = 3 \Rightarrow n = 6, k = 9, r = 3$

- 18 eq., 19 var. $\Rightarrow$ 18 eq., 18 var.

B: $n = 7, k = 10, r = 4 \Rightarrow n = 7, k = 9, r = 4$

- 21 eq., 22 variables $\Rightarrow$ 21 eq., 21 var.

C: $n = 11, k = 10, r = 8 \Rightarrow n = 11, k = 9, r = 8$

- 34 eq., 35 variables $\Rightarrow$ 34 eq., 34 var.

Experimental results with FGb (2008)

$$\mathbb{K} = \mathbb{F}_{65521}$$

	n	k	r	T_{FGb}	Mem	N_{FGb}	[Cou]
A	6	9	3	1 min.	400 Mb.	$2^{30.5}$	2^{106}
B	7	9	4	1h45min.	3 Gb.	$2^{37.1}$	2^{122}
	8	9	5	91 h.	58.5 Gb.	$2^{43.4}$	
C	11	9	8			$2^{64.4}$ "not rigorous"	2^{136}

	n	k	r	d_{reg} (theor.)	d_{reg} (observed)	Bezout	$\#\mathcal{S}ol$
A	6	9	3	19	5	2^{18}	2^{10}
B	7	9	4	22	6	2^{21}	2^{12}
	8	9	5	28	8	2^{27}	2^{13}
C	11	9	8	33	?	2^{34}	?

Efficient attack but no theoretical explanation !!

Multi-Homogeneous Structure

Homogeneous

$f(x_1, \ldots, x_n)$ **homogeneous** of degree $d \Rightarrow$

$$\forall \alpha \in \mathbb{K}, f(\alpha \cdot x_1, \ldots, \alpha \cdot x_n) = \alpha^d f(x_1, \ldots, x_n).$$

Multi-Homogeneous Structure

Homogeneous

$f(x_1, \dots, x_n)$ **homogeneous** of degree $d \Rightarrow$

$$\forall \alpha \in \mathbb{K}, f(\alpha \cdot x_1, \dots, \alpha \cdot x_n) = \alpha^d f(x_1, \dots, x_n).$$

Definition

Let $[X^{(0)}, \dots, X^{(k)}]$ be a partition of the variables.
$f \in \mathbb{K}[X^{(0)}, \dots, X^{(k)}]$ is **multi-homogeneous** of **multi-degree** $d_0, \dots, d_k$ if for all $(\alpha_0, \dots, \alpha_k) \in \mathbb{K}^{k+1}$:

$$f(\alpha_0 \cdot X^{(0)}, \dots, \alpha_k \cdot X^{(k)}) = \alpha_0^{d_0} \cdots \alpha_k^{d_k} f(X^{(0)}, \dots, X^{(k)}).$$

Multi-Homogeneous Structure

Property

The ideal $\mathcal{I}_{\mathrm{KS}}$ is multi-homogeneous ($[Y, X^{(1)}, \ldots, X^{(n-r)}]$).

- new bounds for the degree of regularity
- multi-homogeneous Bézout bound

$$\left(\sum_{j=1}^{k} y_j M_j\right) \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \\ x_1^{(1)} & \cdots & \cdots & x_1^{(n-r)} \\ \vdots & \vdots & \vdots & \vdots \\ x_r^{(1)} & \cdots & \cdots & x_r^{(n-r)} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

Theoretical Complexity

Conjecture

Let $r' = n - r$ be a constant. We consider instances of MR with parameters $\left(n, k = r'^2, r = n - r'\right)$. For those particular instances, we can compute the variety of $\mathcal{I}_{\mathrm{KS}}$ using Gröbner bases in :

$$\mathcal{O}\left(\ln\left(\#\mathbb{K}\right)\, n^{3\,r'^2}\right),$$

The complexity of our attack is polynomial for instances of MinRank with $\left(n, k = r'^2, r = n - r'\right)$.

(n, k, r)	$A = (6, 9, 3)$	$B = (7, 9, 4)$	$C = (11, 9, 8)$
$\#\mathcal{S}ol$ (MH Bézout bound)	2^{13}	2^{15}	2^{22}
Experimental $\#\mathcal{S}ol$	2^{10}	2^{12}	
Complexity bound	$2^{38.9}$	$2^{46.2}$	$2^{66.3}$
Experimental Bound	$2^{30.5}$	$2^{37.1}$	$2^{64.3}$

Theoretical Complexity

J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer. *"Computing Loci of Rank Defects of Linear Matrices using Grbner Bases and Applications to Cryptology."*. ISSAC 2009.

Theorem (Faugère, Safey El Din, Spaenlehauer)

Let (n, r, k) be the parameters of a MinRank instance, $\mathbf{A} = [a_{i,j}]$ be the $(r \times r)$-matrix with $a_{i,j}(t) = \sum_{\ell=0}^{n-\max(i,j)} \binom{n-i}{\ell}\binom{n-j}{\ell} t^{\ell}$. The **degree of regularity** *is $\leq 1 + \deg(\mathrm{HS}(t))$ where $\mathrm{HS}(t)$ is the polynomial obtained from the first positive terms of the series*

$$(1-t)^{(n-r)^2-k}\frac{\det \mathbf{A}(t)}{t^{\binom{r}{2}}}.$$

Theoretical Complexity

L. Bettale, J.-C. Faugère, L. Perret.
"Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants". PKC 2011

Main Results

- Improved key recovery attack on HFE
- Extension of the attack to Multi-HFE
- Practical challenges broken
- Proved theoretical complexity of the attack
- Characterization of equivalent keys
- Attack on Multi-HFE variants.
- Careful recovery of the secret key

Conclusion

Formerly

Algebraic techniques = modeling the problem by algebraic equations + computing a Gröbner basis.

Conclusion

Formerly

Algebraic techniques = modeling the problem by algebraic equations + computing a Gröbner basis.

New trend

Theoretical complexity analysis to explain the behavior of the attack.

- Systematic use of structured systems (algebraic cryptanalysis of code-based systems).

J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer. *“Gröbner Bases of Bihomogeneous Ideals generated by Polynomials of Bidegree (1,1): Algorithms and Complexity".* JSC 2011.