Gröbner Bases. Applications in Cryptology

Jean-Charles Faugère
INRIA, Université Paris 6, CNRS

with partial support of Celar/DGA

FSE 20007 - Luxembourg

Goal: how Gröbner bases can be used to break (block) ciphers ?

1. Basic Properties of Gröbner Bases

Goal: how Gröbner bases can be used to break (block) ciphers ?

1. Basic Properties of Gröbner Bases
2. Use the same benchmark during the talk: non-trivial iterated block ciphers from **"Block Ciphers Sensitive to Gröbner Basis Attacks"**, *J. Buchmann, A. Pyshkin and R.-P. Weinmann, CT-RSA 2006*

Goal: how Gröbner bases can be used to break (block) ciphers ?

1. Basic Properties of Gröbner Bases
2. Use the same benchmark during the talk: non-trivial iterated block ciphers from **"Block Ciphers Sensitive to Gröbner Basis Attacks"**, *J. Buchmann, A. Pyshkin and R.-P. Weinmann, CT-RSA 2006*
3. Efficient algorithms for computing Gröbner Bases

Goal: how Gröbner bases can be used to break (block) ciphers ?

1. Basic Properties of Gröbner Bases
2. Use the same benchmark during the talk: non-trivial iterated block ciphers from **"Block Ciphers Sensitive to Gröbner Basis Attacks"**, *J. Buchmann, A. Pyshkin and R.-P. Weinmann, CT-RSA 2006*
3. Efficient algorithms for computing Gröbner Bases
4. Test different algorithms and strategies: Direct, Substitution of some variables, several plaintexts/ciphertexts.

Properties of Gröbner bases I

$\mathbb{K}$ a field, $\mathbb{K}[x_1,\ldots,x_n]$ polynomials in n variables.

Linear systems	Polynomial equations
$\begin{cases} l_1(x_1,\ldots,x_n)=0 \\ \ldots \\ l_m(x_1,\ldots,x_n)=0 \end{cases}$	$\begin{cases} f_1(x_1,\ldots,x_n)=0 \\ \ldots \\ f_m(x_1,\ldots,x_n)=0 \end{cases}$
$V=\mathrm{Vect}_{\mathbb{K}}(l_1,\ldots,l_m)$	Ideal generated by f_i: $I=\mathrm{Id}(f_1,\ldots,f_m)$
Triangular/diagonal basis of V	Gröbner basis of I

Definition (Buchberger)

$<$ admissible ordering (lexicographical, total degree, DRL)

$G\subset\mathbb{K}[x_1,\ldots,x_n]$ is a Gröbner basis of an ideal I if

$$\forall f\in I,\text{ exists } g\in G \text{ such that } \mathrm{LT}_<(g)\mid\mathrm{LT}_<(f)$$

Properties of Gröbner bases II

Solving algebraic systems:
Computing the algebraic variety: $\mathbb{K} \subset \mathbb{L}$ (for instance $\mathbb{L}=\overline{\mathbb{K}}$ the algebraic closure)

$$V_{\mathbb{L}} = \{(z_1, \ldots, z_n) \in \mathbb{L}^n \mid f_i(z_1, \ldots, z_n) = 0, \quad i = 1, \ldots, m\}$$

Solutions in finite fields:
We compute the Gröbner basis of $G_{\mathbb{F}_2}$ of $[f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n]$, in $\mathbb{F}_2[x_1, \ldots, x_n]$. It is a description of all the solutions of $V_{\mathbb{F}_2}$.

Properties of Gröbner bases III

Theorem

- $V_{\mathbb{F}_2} = \emptyset$ *(no solution) iff* $G_{\mathbb{F}_2} = [1]$.
- $V_{\mathbb{F}_2}$ *has exactly one solution iff* $G_{\mathbb{F}_2} = [x_1 - a_1, \ldots, x_n - a_n]$ *where* $(a_1, \ldots, a_n) \in \mathbb{F}_2^n$.

Shape position:
If $m \geq n$ and the number of solutions is finite ($\#V_K < \infty$), then *in general* the shape of a lexicographical Gröbner basis: $x_1 > \cdots > x_n$:

$$\text{Shape Position} \left\{ \begin{array}{c} h_n(x_n)(=0) \\ x_{n-1} - h_{n-1}(x_n)(=0) \\ \vdots \\ x_1 - h_1(x_n)(=0) \end{array} \right.$$

Feistel cipher: FLURRY I

Flurry(k, t, r, f, D) the parameters used are:

- k *size* of the finite field $\mathbb{K}$.
- t is the *size* of the message/secret key and $m = \frac{t}{2}$ the half size.
- r the *number of rounds*.
- f a non-linear mapping giving the *S-Box* of the round function.

In practice: $f(x) = f_p(x) = x^p$ or $f(x) = f_{\text{inv}}(x) = x^{k-2}$.

- D a $m \times m$ matrix describing the *linear diffusion mapping* of the round function (coefficients in $\mathbb{K}$).

Feistel cipher: FLURRY II

We set $L = [l_1, \ldots, l_m] \in \mathbb{K}^m$ and $R = [r_1, \ldots, r_m]$ the *left/right* side of the current state. and $K = [k_1, \ldots, k_m]$ the *secret key*.
We define the *round function*
$\rho : \mathbb{K}^m \times \mathbb{K}^m \times \mathbb{K}^m \rightarrow \mathbb{K}^m \times \mathbb{K}^m$ as

$$\rho(L, R, K) = (R, D.^T [f(r_1 + k_1), \ldots, f(r_m + k_m)])$$

The key schedule. from an initial secret key $[K_0, K_1]$ (size $t = 2\,m$) we compute subsequent round keys for $2 \leq i \leq r + 1$ as follows:

$$K_i = D.^T K_{i-1} + K_{i-2} + v_i, \quad i = 2, 3, \ldots, (r+1)$$

where v_i are round constants.

Feistel cipher: FLURRY III

A plaintext $[L_0, R_0]$ (size t) is *encrypted* into a ciphertext (L_r, R_r) by iterating the round function ρ over r rounds:

$$\begin{aligned}(L_i, R_i) &= \rho(L_{i-1}, R_{i-1}, K_{i-1}) \quad \text{for} \quad i = 1, 2, \ldots, (r-1)\\ (L_r, R_r) &= \rho(L_{r-1}, R_{r-1}, K_{r-1}) + (0, K_{r+1})\end{aligned}$$

and $L_i = R_{i-1}$.

Feistel cipher: algebraic attack. I

Algebraic attack: The encryption process can be described by very simple polynomial equations: introduce variables for each round $L_j = [x_{1,j}, \ldots, x_{m,j}]$, $R_j = [x_{m+1,j}, \ldots, x_{t,j}]$ and $K_j = [k_{1,j}, \ldots, k_{m,j}] \longrightarrow F$ *algebraic set of equations.*

for
plaintex: $\vec{p} = L_0 \cup R_0$
ciphertext: $\vec{c} = L_{r+1} \cup R_{r+1}$
secret key: $\vec{k} = K_0 \cup K_1$
of size t equations:

$\boxed{\mathcal{S}_{\vec{k}}(\vec{p}, \vec{c})}$ is the corresponding algebraic system

In the following: if $\vec{p}$ is explicitly known then we note $\vec{p}^*$; hence we obtain $\mathcal{S}_{\vec{k}}(\vec{p}^*, \vec{c}^*)$

Feistel cipher: algebraic attack. II

Theorem

[Buchmann, Pyshkin, Weinmann]. If $f(x) = x^p$*, for an appropriate variable order* $x_{i,j}, k_{i,j}$ *then* $\mathcal{S}_{\vec{k}}(\vec{p}^*, \vec{c}^*)$ *is already a Gröbner basis for a total degree ordering.*

Main problem: we are computing $V_{\overline{\mathbb{K}}}$ and not $V_{\mathbb{K}}$!

and *many* solutions: $p^{m\,r}$

Algorithms I

Algorithms: for *computing* Gröbner bases.

- Buchberger (1965,1979,1985)
- F_4 using linear algebra (1999) (strategies)
- F_5 no reduction to zero (2002)

Linear Algebra and Matrices

Trivial link: Linear Algebra $\leftrightarrow$ Polynomials

Definition: $F = (f_1, \ldots, f_m)$, $<$ ordering. A Matrix representation M_F of F is such that

$$^{T}F = M_F . ^{T}X$$

where X all the terms (sorted for $<$) occurring in F:

$$\begin{array}{cc} & m_1 > m_2 > m_3 \\ M_F = \begin{array}{c} f_1 \\ f_2 \\ f_3 \end{array} & \left(\begin{array}{c} \ldots \\ \ldots \\ \ldots \end{array} \right) \end{array}$$

Algorithms II

Linear Algebra and Matrices

Trivial link: Linear Algebra $\leftrightarrow$ Polynomials

If Y is a vector of monomials, M a matrix then its polynomial representation is

$$^T[f_1, \ldots, f_m] = M^T_. Y$$

Macaulay method

Macaulay bound (for homogeneous polynomials):

$$D = 1 + \sum_{i=1}^{m} (deg(f_i) - 1)$$

Algorithms III

We compute the matrix representation of
$\{tf_i,\ deg(t) \leq D - deg(f_i),\ i = 1, \ldots, m\}$, $<_{\mathrm{DRL}}$

$$M_{\mathrm{Mac}} = \begin{array}{c} \\ t_1 f_1 \\ t_1' f_1 \\ t_2' f_2 \\ t_2 f_2 \\ t_3 f_3 \end{array} \begin{array}{c} m_1 > m_2 > m_3 > \cdots > m_r \\ \left(\begin{array}{c} \ldots \\ \ldots \\ \ldots \\ \ldots \\ \ldots \end{array} \right) \end{array}$$

Let $\tilde{M}_{\mathrm{Mac}}$ be the result of *Gaussian elimination*.

Theorem

(Lazard 83) If F is regular then the polynomial representation of $\tilde{M}_{Mac}$ is a Gröbner basis.

Efficient Algorithms

F_4 (1999) linear algebra

Efficient Algorithms

F_4 (1999) linear algebra
Small subset of rows: F_5 (2002) **full rank matrix**

Efficient Algorithms

F_4 (1999) linear algebra
Small subset of rows: F_5 (2002) **full rank matrix** $F_5/2$ (2002) **full rank matrix** GF(2) (includes Frobenius $h^2 = h$)

$$\begin{array}{cc} & \textit{momoms degree } \mathbf{d} \textit{ in } x_1, \ldots, x_n \\ A_d = \begin{array}{c} monom \times f_{i_1} \\ monom \times f_{i_2} \\ monom \times f_{i_3} \end{array} & \left(\begin{array}{c} \ldots \\ \ldots \\ \ldots \end{array} \right) \end{array}$$

F_5 the idea I

We consider the following example: (b parameter):

$$\mathcal{S}_b \begin{cases} f_3 = x^2 + 18\,xy + 19\,y^2 + 8\,xz + 5\,yz + 7\,z^2 \\ f_2 = 3\,x^2 + (7 + \ b)\,x\,y + 22\,x\,z + 11\,yz + 22\,z^2 + 8\,y^2 \\ f_1 = 6\,x^2 + 12\,xy + 4\,y^2 + 14\,xz + 9\,yz + 7\,z^2 \end{cases}$$

With Buchberger $x > y > z$:

- 5 useless reductions
- 5 useful pairs

F_5 the idea II

We proceed degree by degree.

$$A_2 = \begin{array}{c|cccccc|} & x^2 & x\,y & y^2 & x\,z & y\,z & z^2 \\ f_3 & 1 & 18 & 19 & 8 & 5 & 7 \\ f_2 & 3 & 7 & 8 & 22 & 11 & 22 \\ f_1 & 6 & 12 & 4 & 14 & 9 & 7 \end{array}$$

$$\widetilde{A_2} = \begin{array}{c|cccccc|} & x^2 & x\,y & y^2 & x\,z & y\,z & z^2 \\ f_3 & 1 & 18 & 19 & 8 & 5 & 7 \\ f_2 & & 1 & 3 & 2 & 4 & -1 \\ f_1 & & & 1 & -11 & -3 & -5 \end{array}$$

"new" polynomials $f_4 = xy + 4\,yz + 2\,xz + 3\,y^2 - z^2$ and $f_5 = y^2 - 11\,xz - 3\,yz - 5\,z^2$

F_5 the idea III

$$f_3 = x^2 + 18\,xy + 19\,y^2 + 8\,xz + 5\,yz + 7\,z^2$$
$$f_2 = 3\,x^2 + 7x\,y + 22\,x\,z + 11\,yz + 22\,z^2 + 8\,y^2$$
$$f_1 = 6\,x^2 + 12\,xy + 4\,y^2 + 14\,xz + 9\,yz + 7\,z^2$$
$$f_4 = xy + 4\,yz + 2\,xz + 3\,y^2 - z^2$$
$$f_5 = y^2 - 11\,xz - 3\,yz - 5\,z^2$$

$$f_2 \longrightarrow f_4$$
$$f_1 \longrightarrow f_5$$

Degree 3 I

$$
\begin{array}{c|cccccc}
 & x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \\
\hline
zf_3 & 0 & 0 & 0 & 0 & 1 & \dots \\
yf_3 & 0 & 1 & 18 & 19 & 0 & \dots \\
xf_3 & 1 & 18 & 19 & 0 & 8 & \dots \\
zf_2 & 0 & 0 & 0 & 0 & 3 & \dots \\
yf_2 & 0 & 3 & 7 & 8 & 0 & \dots \\
xf_2 & 3 & 7 & 8 & 0 & 22 & \dots \\
zf_1 & 0 & 0 & 0 & 0 & 6 & \dots \\
yf_1 & 0 & 6 & 12 & 4 & 0 & \dots \\
xf_1 & 6 & 12 & 4 & 0 & 14 & \dots
\end{array}
$$

Degree 3 II

$$
\begin{array}{c}
 \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1
\end{array}
\begin{array}{c}
\begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \dots \end{array} \\
\begin{pmatrix}
0 & 0 & 0 & 0 & \boxed{1} & \dots \\
0 & 1 & 18 & 19 & 0 & \dots \\
1 & 18 & 19 & 0 & 8 & \dots \\
0 & 0 & 0 & 0 & \boxed{3} & \dots \\
0 & 3 & 7 & 8 & 0 & \dots \\
3 & 7 & 8 & 0 & 22 & \dots \\
0 & 0 & 0 & 0 & 6 & \dots \\
0 & 6 & 12 & 4 & 0 & \dots \\
6 & 12 & 4 & 0 & 14 & \dots
\end{pmatrix}
\end{array}
$$

Degree 3 III

$$A_3 = \begin{array}{c} \\ zf_3 \\ yf_3 \\ xf_3 \\ zf_2 \\ yf_2 \\ xf_2 \\ zf_1 \\ yf_1 \\ xf_1 \end{array} \begin{array}{c} \begin{array}{cccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & \ldots \end{array} \\ \left(\begin{array}{cccccc} 0 & 0 & 0 & 0 & \textcircled{1} & \ldots \\ 0 & 1 & 18 & 19 & 0 & \ldots \\ 1 & 18 & 19 & 0 & 8 & \ldots \\ 0 & 0 & 0 & 0 & \textcircled{3} & \ldots \\ 0 & 3 & 7 & 8 & 0 & \ldots \\ 3 & 7 & 8 & 0 & 22 & \ldots \\ 0 & 0 & 0 & 0 & 6 & \ldots \\ 0 & 6 & 12 & 4 & 0 & \ldots \\ 6 & 12 & 4 & 0 & 14 & \ldots \end{array}\right) \end{array}$$

Degree 3 IV

$$f_2 \longrightarrow f_4$$

$$f_1 \longrightarrow f_5$$

	x^3	x^2y	xy^2	y^3	x^2z	$\dots$
zf_3	0	0	0	0	1	$\dots$
yf_3	0	1	18	19	0	$\dots$
xf_3	1	18	19	0	8	$\dots$
zf_2	0	0	0	0	3	$\dots$
yf_2	0	3	7	8	0	$\dots$
xf_2	3	7	8	0	22	$\dots$
zf_1	0	0	0	0	6	$\dots$
yf_1	0	6	12	4	0	$\dots$
xf_1	6	12	4	0	14	$\dots$

Degree 3 V

$$\widetilde{A_3} = \begin{array}{c} \\ z\,f_3 \\ y\,f_3 \\ x\,f_3 \\ z\,f_4 \\ y\,f_4 \\ x\,f_4 \\ z\,f_5 \\ y\,f_5 \\ x\,f_5 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 \end{array} \\ \left(\begin{array}{cccccccccc} 0 & 0 & 0 & 0 & 1 & 18 & 19 & 8 & 5 & 7 \\ 0 & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\ 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 & 2 & 4 & 22 \\ 0 & 0 & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\ 0 & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 12 & 20 & 18 \\ 0 & 0 & 0 & 1 & 0 & 12 & 20 & 0 & 18 & 0 \\ 0 & 0 & 1 & 0 & 12 & 20 & 0 & 18 & 0 & 0 \end{array}\right) \end{array}$$

We have constructed 3 new polynomials

$$\begin{aligned} f_6 &= y^3 + 8\,y^2z + xz^2 + 18\,yz^2 + 15\,z^3 \\ f_7 &= xz^2 + 11\,yz^2 + 13\,z^3 \\ f_8 &= yz^2 + 18\,z^3 \end{aligned}$$

We have the linear equivalences: $x\,f_2 \leftrightarrow x\,f_4 \leftrightarrow f_6$ and $f_4 \longrightarrow f_2$

Degree 4: reduction to 0 !

The matrix whose rows are

$$x^2 f_i, x\,y f_i, y^2 f_i, x\,z f_i, y\,z f_i, z^2 f_i, \quad i = 1, 2, 3$$

is not full rank !

Why ?

$6 \times 3 =$ $\boxed{\text{18 rows}}$

but only $x^4, x^3\, y, \ldots, y\, z^3, z^4$ $\boxed{\text{15 columns}}$

Simple linear algebra theorem: 3 useless row (which ones ?)

Trivial relations

$$f_2\, f_3 - f_3\, f_2 = 0$$

can be rewritten

$$3\,x^2\, f_3 + (7 + \ b)\, xy\, f_3 + 8\, y^2\, f_3 + 22\, xz\, f_3$$
$$+11\, yz\, f_3 + 22\, z^2\, f_3 - \boxed{x^2\, f_2} - 18\, xy\, f_2 - 19\, y^2\, f_2$$
$$-8\, xz\, f_2 - 5\, yz\, f_2 - 7\, z^2\, f_2 = 0$$

We can remove the row $x^2 f_2$

same way $f_1 f_3 - f_3 f_1 = 0 \longrightarrow$ remove $x^2 f_1$

but $f_1 f_2 - f_2 f_1 = 0 \longrightarrow$ remove $x^2 f_1$! ???

Combining trivial relations

$$
\begin{aligned}
0 &= (f_2 f_1 - f_1 f_2) - 3(f_3 f_1 - f_1 f_3) \\
0 &= (f_2 - 3f_3) f_1 - f_1 f_2 + 3 f_1 f_3 \\
0 &= f_4 f_1 - f_1 f_2 + 3 f_1 f_3 \\
0 &= ((1 - b)xy + 4\,yz + 2\,xz + 3\,y^2 - z^2)\, f_1 \\
&\quad -(6x^2 + \cdots) f_2 + 3(6x^2 + \cdots) f_3
\end{aligned}
$$

- if $b \neq 1$ remove $x\,y\;f_1$
- if $b = 1$ remove $y\,z\;f_1$

Need “some” computation

New Criterion

Any combination of the trivial relations $f_i f_j = f_j f_i$ can always be written:

$$u(f_2 f_1 - f_1 f_2) + v(f_3 f_1 - f_1 f_3) + w(f_2 f_3 - f_3 f_2)$$

where u, v, w are arbitrary polynomials.

$$(u\, f_2 + v\, f_3)\, f_1 - u f_1 f_2 - v f_1 f_3 + w f_2 f_3 - w f_3 f_2$$

(trivial) relation $h f_1 + \cdots = 0 \leftrightarrow \; h \in \mathrm{Id}(f_2, f_3)$

Compute a Gröbner basis of $(f_2, f_3) \longrightarrow G_{\text{prev}}$.

Remove line $h\, f_1$ iff $\mathrm{LT}(h)$ top reducible by G_{prev}

Degree 4 I

$$y^2 f_1, x\,zf_1, y\,zf_1, z^2 f_1, x\,yf_2, y^2 f_2, x\,zf_2,$$
$$y\,zf_2, z^2 f_2, x^2 f_3, x\,yf_3, y^2 f_3, x\,zf_3, y\,zf_3, z^2 f_3$$

In order to use previous computations (degree 2 and 3):

$$\begin{array}{cc} xf_2 \longrightarrow f_6 & f_2 \longrightarrow f_4 \\ xf_1 \longrightarrow f_8 & yf_1 \longrightarrow f_7 \\ f_1 \longrightarrow f_5 & \end{array}$$

$$yf_7, zf_8, zf_7, z^2 f_5, yf_6, y^2 f_4, zf_6, y\,zf_4,$$
$$z^2 f_4, x^2 f_3, x\,yf_3, y^2 f_3, x\,zf_3, y\,zf_3, z^2 f_3,$$

Degree 4 II

$$
\begin{bmatrix}
1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 & & 1 & 18 & 19 & 0 & 0 & 8 & 5 & 0 & 0 & 7 & 0 & 0 & 0 \\
 & & & 1 & 3 & 0 & 0 & 2 & 4 & 0 & 0 & 22 & 0 & 0 & 0 \\
 & & & & 1 & 0 & 0 & 0 & 8 & 0 & 1 & 18 & 0 & 15 & 0 \\
 & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 & 0 \\
 & & & & & & 1 & 18 & 19 & 0 & 8 & 5 & 0 & 7 & 0 \\
 & & & & & & & 1 & 3 & 0 & 2 & 4 & 0 & 22 & 0 \\
 & & & & & & & & 1 & 0 & 0 & 8 & 1 & 18 & 15 \\
 & & & & & & & & & 1 & 18 & 19 & 8 & 5 & 7 \\
 & & & & & & & & & & 1 & 11 & 0 & 13 & 0 \\
 & & & & & & & & & & & 1 & 12 & 20 & 18 \\
 & & & & & & & & & & & & 1 & 11 & 13 \\
 & & & & & & & & & & & & & 1 & 18 \\
 & & & & & & & & & & 1 & 3 & 2 & 4 & 22
\end{bmatrix}
$$

Degree 4 III

Sub matrix:

$$\begin{array}{c} \\ z^2 f_4 \\ z^2 f_5 \\ z f_7 \\ z f_8 \\ y f_7 \end{array}
\begin{array}{c} \begin{array}{ccccc} xyz^2 & y^2z^2 & xz^3 & yz^3 & z^4 \end{array} \\
\left(\begin{array}{ccccc} 1 & 3 & 2 & 4 & 22 \\ & 1 & 12 & 20 & 18 \\ & & 1 & 11 & 13 \\ & & & 1 & 18 \\ 1 & 11 & 0 & 13 & 0 \end{array} \right) \end{array}$$

New algorithm

- Incremental algorithm

$$(f) + G_{\text{old}}$$

- Incremental degree by degree
- Give a "unique name" to each row

Remove $h\, f_1 + \cdots$ if $\mathrm{LT}(h) \in \mathrm{LT}(G_{\text{old}})$

$\mathrm{LT}(h)$ signature/index of the row

F_5 matrix

Special/Simpler version of F_5 for dense/generic polynomials.
the maximal degree D is a *parameter* of the algorithm.
degree d $m = 2$, $\deg(f_i) = 2$ homogeneous quadratic polynomials, degree d:

We may assume that we have already computed:

$G_{i,d}$ Gröbner basis $[f_1, \ldots, f_i]$ up do degree d

In degree d

$$
\begin{array}{c}
 \\ u_1 f_1 \\ u_2 f_1 \\ u_3 f_1 \\ v_1 f_2 \\ v_2 f_2 \\ w_1 f_3 \\ w_2 f_3 \\ \vdots
\end{array}
\begin{array}{c}
\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \ldots \end{array} \\
\begin{pmatrix}
1 & x & x & x & x & \ldots \\
0 & 1 & x & x & x & \ldots \\
0 & 0 & 1 & x & x & \ldots \\
0 & 0 & 0 & 1 & x & \ldots \\
0 & 0 & 0 & 0 & 1 & \ldots \\
0 & 0 & 0 & 0 & 0 & \ldots \\
0 & 0 & 0 & 0 & 0 & \ldots \\
0 & 0 & 0 & 0 & 0 & \vdots
\end{pmatrix}
\end{array}
$$

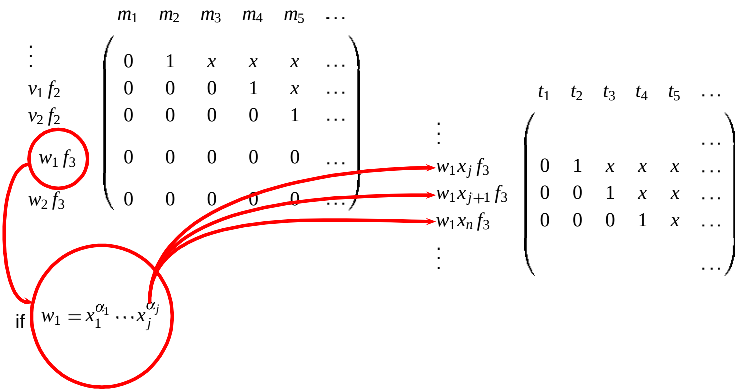
with $\deg(u_i) = \deg(v_i) = \deg(w_i) = d - 2$

From degree d to $d+1$ I

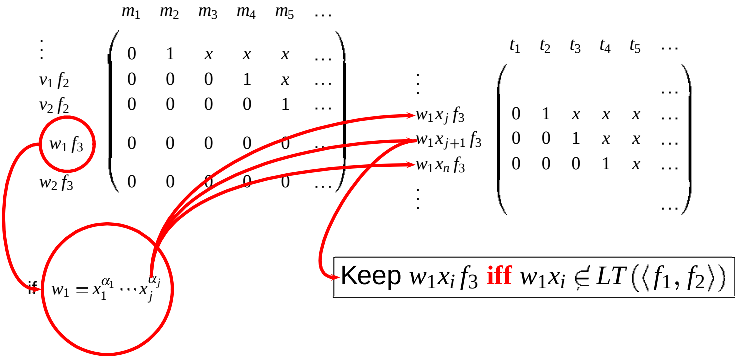
Select a row in degree d:

$$\begin{array}{c} \\ \vdots \\ v_1 f_2 \\ v_2 f_2 \\ \textcircled{w_1 f_3} \\ w_2 f_3 \end{array} \begin{array}{c} \begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \ldots \end{array} \\ \left(\begin{array}{cccccc} 0 & 1 & x & x & x & \ldots \\ 0 & 0 & 0 & 1 & x & \ldots \\ 0 & 0 & 0 & 0 & 1 & \ldots \\ 0 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 0 & 0 & \ldots \end{array}\right) \end{array}$$

From degree d to $d+1$ II



From degree d to $d+1$ III



From degree d to $d+1$ IV

$$
\begin{array}{c}
\vdots \\ v_1 f_2 \\ v_2 f_2 \\ w_1 f_3 \\ w_2 f_3
\end{array}
\begin{array}{c}
\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \dots \end{array} \\
\begin{pmatrix}
0 & 1 & x & x & x & \dots \\
0 & 0 & 0 & 1 & x & \dots \\
0 & 0 & 0 & 0 & 1 & \dots \\
0 & 0 & 0 & 0 & 0 & \dots \\
0 & 0 & 0 & 0 & 0 & \dots
\end{pmatrix}
\end{array}
\qquad
\begin{array}{c}
\vdots \\ w_1 x_j f_3 \\ w_1 x_{j+1} f_3 \\ w_1 x_n f_3 \\ \vdots
\end{array}
\begin{array}{c}
\begin{array}{cccccc} t_1 & t_2 & t_3 & t_4 & t_5 & \dots \end{array} \\
\begin{pmatrix}
 & & & & & \dots \\
0 & 1 & x & x & x & \dots \\
0 & 0 & 1 & x & x & \dots \\
0 & 0 & 0 & 1 & x & \dots \\
 & & & & & \dots
\end{pmatrix}
\end{array}
$$

if $w_1 = x_1^{\alpha_1} \cdots x_j^{\alpha_j}$

Keep $w_1 x_i f_3$ **iff** $w_i x_i$ not reducible by $\mathrm{LT}(G_{2,d-2})$

F_5 properties

Full version of F_5 : D the maximal degree is *not given*.

Theorem If $F = [f_1, \ldots, f_m]$ is a (semi) regular sequence then all the matrices are full rank.

- Easy to adapt for the special case of $\mathbb{F}_2$ (*new trivial syzygy:* $f_i^2 = f_i$).
- Incremental in degree/equations (swap 2 loops)
- Fast in general (but not always)
- F_5 matrix: easy to implement, used in applications (HFE).

FLURRY: first step

Flurry	$\dim(I)$	Magma 2.11 F_4	Magma 2.13 F_4	FGb F_5
t=2 r=4 x^5	625	0s	0s	0s
t,r,x^p	$p^{r\frac{t}{2}}$	0s	0s	0s
t=4 r=4 x^3	6521	0s	0s	0s
t=2 r=10 x^{-1}	221	22.1 s	10.7 s	0.8 s
t=2 r=12 x^{-1}	596	×	209.8 s	9.1 s
t=4 r=5 x^{-1}	274	26.0 s	14.3 s	1.2 s
t=4 r=6 x^{-1}	1126	×	902 s	46.9 s
t=6 r=4 x^{-1}	583	×	83 s	12.2s
Rand 20,40	1			365s

CPU Time: Gröbner DRL

Solving zero-dimensional system

When $\dim(I) = 0$ (finite number of solutions); in general:

- It is easier to compute a Gröbner Basis of I for a total degree ($<_{\text{DRL}}$) ordering
- Triangular structure of Gb valid only for a lex. ordering:

$$\text{Shape Position} \begin{cases} h_n(x_n) = 0 \\ x_{n-1} = h_{n-1}(x_n) \\ \vdots \\ x_1 = h_1(x_n) \end{cases}$$

Dedicated Algorithm: efficiently change the ordering

FGLM, Gröbner Walk, LLL, ...

FGLM

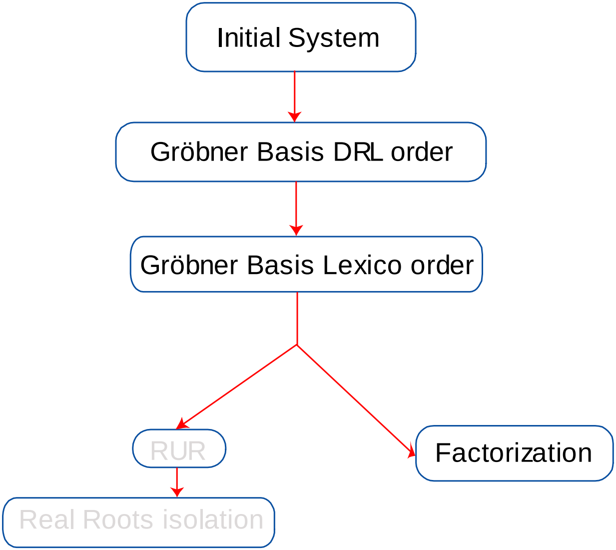
Dedicated Algorithm: efficiently change the ordering

FGLM = use only linear algebra.

Theorem (FGLM)

If $\dim(I) = 0$ and D=$\deg(I)$. Assume that G a Gröbner basis of I is already computed, then G_{new} a Gröbner basis for the same ideal I and a new ordering $<_{new}$ can be computed in $O(n\,D^3)$.

Zero dim solve



Solving FLURRY

Flurry	Dim	Magma 2.11 FGLM	Magma 2.13 FGLM	FGb FGLM
t=2 r=4 x^5	625	8.9s	6.9s	0.6 s
t=2 r=5 x^3	243	0.96s	0.57s	0.07s
t=2 r=6 x^3	729	22.2s	14.5s	1.5s
t=2 r=7 x^3	2187	Out of memory	Out of memory	34.2s
t=4 r=4 x^3	6521	Out of memory	Out of memory	991s
t=2 r=10 x^{-1}	221	24.0 s	10.7 s	1.1 s
t=2 r=12 x^{-1}	596	×	262.3 s	15.1 s
t=4 r=5 x^{-1}	274	34.3 s	21.8 s	2.0 s
t=4 r=6 x^{-1}	1126	×	20 m 35	1 m 21
t=6 r=4 x^{-1}	583	×	441.2s	26.8s

Untractable systems for large t, r

For $x \longmapsto x^p$ the complexity is $O\left(p^{\frac{3}{2}\, m\, r}, \#\mathbb{K}\right)$ and $\beta \leq 9$.

Substitution of 1 variable

Compute a Gröbner basis of $I + \langle x_n - \alpha \rangle$ for some $\alpha \in \mathbb{K}$ (finite field).

Now we have an overdetermined algebraic system and only 1 or 0 solution !

$$\boxed{\text{DRL} + \text{FGLM}} \overset{?}{\longleftrightarrow} \boxed{(\#\mathbb{K})\,(\text{CPU overdetermined})}$$

Substitution of 1 variable

		Magma 2.13	FGb
Flurry	dim(I)	F_4	F_5
t=4 r=4 x^3	6521	1.5 s	0.21 s
t=4 r=6 x^{-1}	1126	6.0 s	0.39 s
t=6 r=4 x^{-1}	583	0.22 s	0.10 s

CPU Time: Gröbner overdetermined

to be compared with:

		Magma 2.13	FGb
Flurry	Dim	FGLM	FGLM
t=4 r=4 x^3	6521	Out of memory	991s
t=4 r=6 x^{-1}	1126	20 m 35	1 m 21
t=6 r=4 x^{-1}	583	441.2s	26.8s

CPU Time: Gröbner DRL + FGLM

Substitution of 1 variable

		FGb	FGb
Flurry	$\dim(I)$	FGLM	F_5
t=4 r=4 x^3	6521	991s	0.21 s
t=4 r=6 x^{-1}	1126	1 m 21	0.39 s
t=6 r=4 x^{-1}	583	26.8s	0.10 s

CPU Time: Gröbner overdetermined

Hence the second method is more efficient

$$\text{if } \#\mathbb{K} \leq \frac{60+21}{0.39} \approx \boxed{136} \text{ for FGb}$$
$$\text{if } \#\mathbb{K} \leq \frac{20*60+35}{6.0} \approx \boxed{206} \text{ for Magma 2.13-10}$$

the complexity is $O\left((\#\mathbb{K})^2\right)$

Several plaintexts I

We choose randomly several plaintexts: $\vec{p}_1^*, \ldots, \vec{p}_N^*$ and we assume that we known the corresponding ciphertex: $\vec{c}_i^*$
We obtain an algebraic system:

$$\mathcal{S}_N = \bigcup_{i=1}^{N} \mathcal{S}_{\vec{k}}(\vec{p}_i^*, \vec{c}_i^*)$$

It is much more difficult to compute the Gröbner basis:

N Nb of plain/cipher text	1	2	3
CPU	0.43 s	25.8s	16m42s
Nb of solutions	184	1	1

$\mathbb{K} = GF(2^7)$, $t = 4$, $f = f_{\text{inv}}$

Same behavior if we fix $k_{1\,0}$ (1 component of the secret key):

Several plaintexts II

N Nb of plain/cipher text	1	2	5	10
CPU	0.01s	0.09s	2.3s	99.5sc
Nb of solutions	1	1	1	1

$\mathbb{K} = GF(2^7)$, $t = 4$, $f = f_{\mathrm{inv}}$, substitution of 1 variable

Chosen plaintexts

Notation: $\vec{e}_i = [\ldots, 0, 1, 0, \ldots]$ canonical basis of $\mathbb{K}^t$. From an initial message:

$$\vec{p}_0^* = [p_{0,1}, \ldots, p_{0,t}]$$

we can construct a new set of messages; for instance for $i = 2$ to N:

$$\vec{p}_i^* = \vec{p}_j^* + \vec{e}_k \quad \text{with} \quad j < i,\ 1 \leq k \leq t$$

We obtain an algebraic system:

$$\mathcal{S}_N = \bigcup_{i=1}^{N} \mathcal{S}_{\vec{k}}(\vec{p}_i^*, \vec{c}_i^*)$$

Experimental results: up to 6 rounds

N	1	2	3	5
FGb CPU	137 s	0.08 sec		
Nb of solutions	583	1	1	1

$\mathbb{K} = GF(65521)$, $t = 6$, $f = f_{\mathrm{inv}}$, $r = 4$.

N	2	3	4	5	6
FGb CPU	$\times$	502 s	8.9s	5.2s	12.2s
Nb of sols	$\times$	1	1	1	1

$\mathbb{K} = GF(2^7)$, $t = 6$, $f = f_{\mathrm{inv}}$, $r = 5$.

N	1	2	3	5
FGb CPU	> 2 h	710.6 s		
Nb of solutions	?	1	1	1

$\mathbb{K} = GF(65521)$, $t = 6$, $f = f_{\mathrm{inv}}$, $r = 6$.

Degree in Gb computation bounded: complexity $O\left((t\, r)^{\beta}\right)$?

And after 7 rounds ?

N	1	2	18	19	20
Nb of solutions	6561	1	1	1	1
F_4 CPU	0 s	980.9s	152s	208.4s	175.9s

$$\mathbb{K} = GF(2^7),\ t = 2,\ \boxed{f = x^3},\ r = 8.$$

But *does not work* for the inverse function !

N	1	3	12	20	50
Nb of sols	46	1	1	1	1
$D_{\max}$	5	4	4	4	4
F_4 CPU	0.07s	3.9s	$\times$	> 293s	> 6527s

$$\mathbb{K} = GF(65521),\ t = 2,\ \boxed{f = x^{-1}},\ r = 7.$$

The attack fails for the inverse function !

Conclusion

- One test example: **Flurry**(k, m, r, f, D) *Buchmann, Pyshkin, Weinmann*
- Several efficient algorithms for computing Gröbner Bases: F_4, F_5, *FGLM*
- Several implementations: Magma, FGb, Singular, ...
- Different strategies: Direct, Substution of some variables, chosen plaintexts
  - *Direct computation*: Gb + FGLM $O\left(p^{\frac{3}{2}\,m\,r}, \#\mathbb{K}\right)$
  - *Chosen plaintexts*:
    - Flurry broken (?) when $f = x^3$ and chosen plaintexts, complexity $O\left((t\,r)^{\beta}, \#\mathbb{K}\right)$ and $\beta \leq 9$.
    - The attack does not work for $f = \frac{1}{x}$ (or too big)