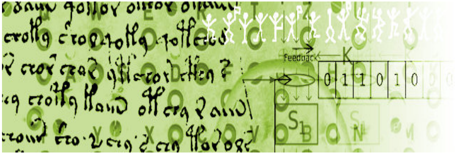
Gröbner Bases in Public-Key Cryptography
An Overview

Ludovic Perret
(joint work with Jean-Charles Faugère)

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

SAGE Days 2007 – University of Bristol

Gröbner Bases in Cryptography ?



C.E. Shannon

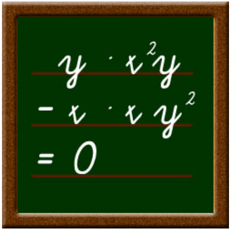
“Breaking a good cipher should require as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type.”
(Communication Theory of Secrecy Systems, 1949)

Algebraic Cryptanalysis

Principle

- Convert a cryptosystem into a set of algebraic equations
- Try to solve this system

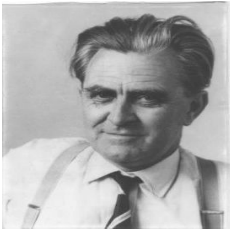
  or estimate the difficulty of the solving step



Solving

Approach

- Using the cryptographic context
- Gröbner Bases
  - Efficient algorithms for computing these bases
    - F_4&F_5 (J.-C. Faugère)



W. Gröbner

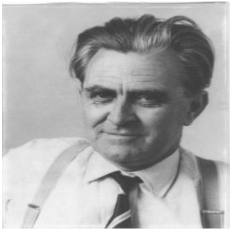
B. Buchberger

J.-C. Faugère

Solving

Approach

- Using the cryptographic context
- Gröbner Bases
  - Efficient algorithms for computing these bases
    - F_4&F_5 (J.-C. Faugère)



W. Gröbner

B. Buchberger

J.-C. Faugère

Algebraic Cryptanalysis in Practice

Difficulties

- Model a cryptosystem as a set of algebraic of 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

Applications

- Algebraic cryptanalysis of block-ciphers
  - AES
- Algebraic aspects of stream ciphers
  - E_0 : mobile phone
- Algebraic cryptanalysis of hash functions ????
  - SHA1
- Multivariate Schemes

Algebraic Cryptanalysis in Practice

Difficulties

- Model a cryptosystem as a set of algebraic of equations

  “universal" approach (PoSSo is NP-Hard)

  ⇒ several models are possible !!!

- Solving

  ⇒ Minimize the number of variables/degree

  ⇒ Maximize the number of equations

Roadmap

(1.) Algebraic Cryptanalysis of HFE

(2.) The IP Problem

(3.) Functional Decomposition

Outline

Multivariate Public-Key Cryptography

General Idea

Let $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]^m$ be s. t. $\forall \mathbf{c} = (c_1, \ldots, c_m) \in \mathbb{K}^m$:

$$V_{\mathbb{K}}\big(\langle f_1 - c_1, \ldots, f_m - c_m \rangle\big),$$

can be computed efficiently.

Secret key :
$(S, U) \in GL_n(\mathbb{K}) \times GL_n(\mathbb{K})$ & $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]^m$

Public key :

$$\mathbf{p}(\mathbf{x}) = \big(p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})\big) = \big(f_1(\mathbf{x} \cdot S), \ldots, f_m(\mathbf{x} \cdot S)\big) U = \mathbf{f}(\mathbf{x} \cdot S) \cdot U,$$

with $\mathbf{x} = (x_1, \ldots, x_n)$.

Encryption

- To encrypt $\mathbf{m} \in \mathbb{K}^n$, compute :

$$\mathbf{c} = \mathbf{p}(\mathbf{m}) = \big(p_1(\mathbf{m}), \ldots, p_m(\mathbf{m})\big).$$

- To decrypt, compute $\mathbf{m}' \in \mathbb{K}^n$ s.t. :

$$\mathbf{f}(\mathbf{m}') = \mathbf{c} \cdot U^{-1}.$$

We then have $\mathbf{m} = \mathbf{m}' \cdot S^{-1}$, if $\# V_{\mathbb{K}}\big(\langle \mathbf{f} - \mathbf{c} \cdot U^{-1} \rangle\big) = 1$.

Proof.

$$\mathbf{p}(\mathbf{m}' \cdot S^{-1}) = \mathbf{f}(\mathbf{m}' \cdot S^{-1} \cdot S) \cdot U = \mathbf{c} \cdot U^{-1} \cdot U = \mathbf{c}.$$

□

Signature

- To verify the signature $\mathbf{s} \in \mathbb{K}^n$ of a digest $\mathbf{m} \in \mathbb{K}^m$:

$$\mathbf{p}(\mathbf{s}) = \mathbf{m}.$$

- To generate $\mathbf{s} \in \mathbb{K}^n$ from a digest $\mathbf{m} \in \mathbb{K}^m$, we apply the decryption process to $\mathbf{m}$, i.e. we compute $\mathbf{s}' \in \mathbb{K}^n$ s.t. :

$$\mathbf{f}(\mathbf{s}') = \mathbf{m} \cdot U^{-1}.$$

The signature is then $\mathbf{s} = \mathbf{s}' \cdot S^{-1}$.

Proof.

$$\mathbf{p}(\mathbf{s}) = \mathbf{f}(\mathbf{s}' \cdot S^{-1} \cdot S) \cdot U = \mathbf{m} \cdot U^{-1} \cdot U = \mathbf{m}.$$

□

The HFE scheme

Secret key :

- $(S, U) \in GL_n(\mathbb{K}) \times GL_n(\mathbb{K})$
- $F = \sum_{i,j} \beta_{i,j} X^{q^{\theta_{i,j}} + q^{\theta'_{i,j}}} \in \mathbb{K}'[X]$, with $\mathbb{K}' \supset \mathbb{K}$, $q = \mathrm{Char}(\mathbb{K})$
- $\mathbf{f} = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \in \mathbb{K}[x_1, \ldots, x_n]^u$

Public key : $(p_1(\mathbf{x}), \ldots, p_n(\mathbf{x})) = (p_1(\mathbf{x} \cdot S), \ldots, p_n(\mathbf{x} \cdot S)) \cdot U$, with $\mathbf{x} = (x_1, \ldots, x_n)$.

J. Patarin.
Hidden Fields Equations (HFE) and Isomorphism of Polynomials (IP): two new families of Asymmetric Algorithms.
EUROCRYPT 1996.

Message Recovery Attack – (I)

Given $\mathbf{c} = (p_1(\mathbf{m}), \ldots, p_n(\mathbf{m})) \in \mathbb{K}^n$. Find $\mathbf{z} \in \mathbb{K}^n$ such that :

$$p_1(\mathbf{z}) - c_1 = 0, \ldots, p_n(\mathbf{z}) - c_n = 0.$$

In Theory ...

- PoSSo is NP-Hard
- Complexity of F_5 for *semi-reg. sys.* : $\mathcal{O}\left(n^{\omega \cdot d_{reg}}\right)$, with :

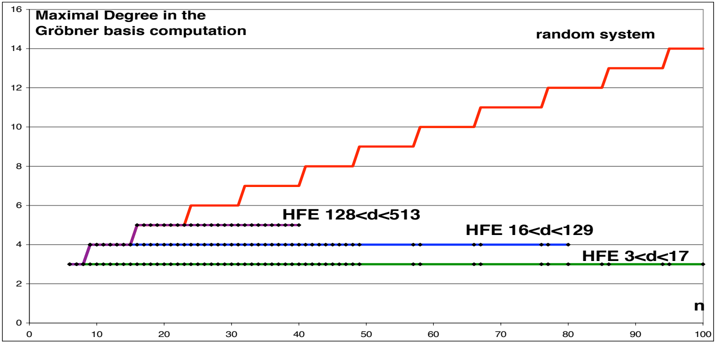
$$d_{reg} \sim \left(-\alpha + \frac{1}{2} + \frac{1}{2}\sqrt{2\alpha^2 - 10\alpha - 1 + 2(\alpha+2)\sqrt{\alpha(\alpha+2)}}\right) n,$$

$\Rightarrow$ For a quadratic system of 80 variables : $d_{reg} = 11$.

$\approx 2^{83}$

Message Recovery Attack – (II)

In Practice . . .



Message Recovery Attack – (II)

In Practice . . .

It has been observed that :

$$d_{reg} = \mathcal{O}\big(\log(D)\big).$$

J.-C. Faugère, A. Joux.
Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases.
CRYPTO 2003.

Outline

"Key Recovery Attack"

IP [J. Patarin, EUROCRYPT 1996]

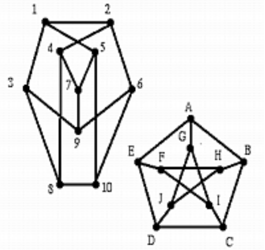
Given : $\mathbf{a} = (a_1, \ldots, a_u)$, and $\mathbf{b} = (b_1, \ldots, b_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$.
Question : Find $(S, U) \in GL_n(\mathbb{K}) \times GL_u(\mathbb{K})$ s. t. :

$$\big(b_1(\mathbf{x}), \ldots, b_u(\mathbf{x})\big) = \big(a_1(\mathbf{x} \cdot S), \ldots, a_u(\mathbf{x} \cdot S)\big) \cdot U,$$

denoted by $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x} \cdot S) \cdot U$, with $\mathbf{x} = (x_1, \ldots, x_n)$.

A Fundamental Problem

O. Billet, H. Gilbert.
A Traceable Block Cipher.
ASIACRYPT 2003.



Basic Idea – (I)

Fact

Suppose that $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x} \cdot S) \cdot U$, *for* $(S, U) \in GL_n(\mathbb{K}) \times GL_u(\mathbb{K})$.
For each i, $1 \leq i \leq u$, *there exist* $E_i \subset \mathbb{K}^n$, *and* p_{α_i} *s. t. :*

$$\left(\mathbf{b}(\mathbf{x}) \cdot U^{-1} - \mathbf{a}(\mathbf{x} \cdot S)\right)_i = \sum_{\alpha_i = (\alpha_{i,1}, \ldots, \alpha_{i,n}) \in E_i} p_{\alpha_i}(S, U^{-1}) x_1^{\alpha_{i,1}} \cdots x_n^{\alpha_{i,n}},$$

where $p_{\alpha_i}(S, U^{-1}) = p_{\alpha_i}(s_{1,1}, \ldots, s_{n,n}, u'_{1,1}, \ldots, u'_{u,u})$.

J.-C. Faugère, L. P.
Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects.
EUROCRYPT 2006.

Basic Idea – (II)

Remark

If $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x} \cdot S) \cdot U$, for some $(S, U) \in GL_n(\mathbb{K}) \times GL_u(\mathbb{K})$, then for all $i, 1 \leq i \leq u$: $\left(\mathbf{b}(\mathbf{x}) \cdot U^{-1} - \mathbf{a}(\mathbf{x} \cdot S)\right)_i =$

$$\sum_{\alpha_i=(\alpha_{i,1},\ldots,\alpha_{i,n})\in E_i} p_{\alpha_i}(S, U^{-1}) x_1^{\alpha_{i,1}} \cdots x_n^{\alpha_{i,n}} = 0.$$

Thus, for all $i, 1 \leq i \leq u$, and for all $\alpha_i \in E_i$:

$$p_{\alpha_i}(S, U^{-1}) = 0.$$

Basic Idea – (III)

Lemma

Let $\mathcal{I} = \langle p\alpha_i, \forall i, 1 \leq i \leq u, \text{ and } \forall \alpha_i \in E_i \rangle$, *and :*

$$V_{\mathbb{K}}(\mathcal{I}) = \left\{ \mathbf{s} \in \mathbb{K}^{n^2+u^2} : p\alpha_i(\mathbf{s}) = 0, \forall 1 \leq i \leq u, \text{ and } \forall \alpha_i \in E_i \right\}.$$

If $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x} \cdot S) \cdot U$, *for some* $(S, U) \in GL_n(\mathbb{K}) \times GL_u(\mathbb{K})$, *then :*

$$\left(\phi_1(S), \phi_2(U^{-1})\right) \in V_{\mathbb{K}}(\mathcal{I}),$$

with :

$$\phi_1 : S = \{s_{i,j}\}_{1 \leq i,j \leq n} \mapsto (s_{1,1}, \ldots, s_{1,n}, \ldots, s_{n,1}, \ldots, s_{n,n}),$$
$$\phi_2 : U^{-1} = \{u'_{i,j}\}_{1 \leq i,j \leq u} \mapsto (u'_{1,1}, \ldots, u'_{1,u}, \ldots, u'_{u,1}, \ldots, u'_{u,u}).$$

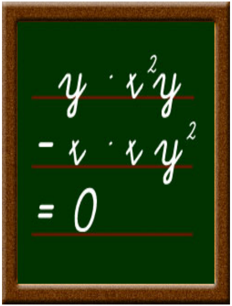
Summary

If $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x} \cdot S) \cdot U$, for $(S, U) \in GL_n(\mathbb{K}) \times GL_u(\mathbb{K})$, then for all i, $1 \leq i \leq u$, $\left(\mathbf{b}(\mathbf{x}) \cdot U^{-1} - \mathbf{a}(\mathbf{x} \cdot S)\right)_i =$

$$\sum_{\alpha_i=(\alpha_{i,1},\ldots,\alpha_{i,n})\in S_i} p_{\alpha_i}(S, U^{-1}) x_1^{\alpha_{i,1}} \cdots x_n^{\alpha_{i,n}} = 0.$$

For all i, $1 \leq i \leq u$, let d_i be the total deg. of a_i.

- at most $\sum_{i=1}^{u} \mathrm{C}_{n+d_i}^{d_i}$ equations
- $n^2 + u^2$ unknowns



A Structural Property

Lemma

Let d be a positive integer, and $\mathcal{I}_d$ be the ideal generated by the polynomials p_{α_i} of maximal total degree smaller than d. If $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x} \cdot S) \cdot U$, for $(S, U) \in GL_n(\mathbb{K}) \times GL_u(\mathbb{K})$, then :

$$\left(\phi_1(S), \phi_2(U^{-1})\right) \in V_{\mathbb{K}}(\mathcal{I}_d), \text{ for all } d, 0 \leq d \leq D,$$

with:

$$\phi_1 : S = \{s_{i,j}\}_{1 \leq i,j \leq n} \mapsto (s_{1,1}, \ldots, s_{1,n}, \ldots, s_{n,1}, \ldots, s_{n,n}), \text{ and}$$
$$\phi_2 : U^{-1} = \{u'_{i,j}\}_{1 \leq i,j \leq u} \mapsto (u'_{1,1}, \ldots, u'_{1,u}, \ldots, u'_{u,1}, \ldots, u'_{u,u}).$$

The IP Algorithm

Input : $(\mathbf{a}, \mathbf{b}) \in \mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^u$
Output : $(S, U) \in GL_n(\mathbb{K}) \times GL_u(\mathbb{K})$, s.t. $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x} \cdot S) \cdot U$ or $\emptyset$

Let $d_0 = \min\{d > 1 : \mathbf{a}^{(d)} \neq \mathbf{0_u}\}$

- **Construct** the $p\alpha_i s$ of max. total degree smaller than d_0
- **Set**

$$\mathcal{I}_{d_0} = \langle p\alpha_i, \forall i, 1 \leq i \leq u, \text{ and } \forall \alpha_i \in E_i : \deg(p\alpha_i) \leq d_0 \rangle.$$

- **Compute** $V_{\mathbb{K}}(\mathcal{I}_{d_0})$ (in practice $V_{\overline{\mathbb{K}}}(\mathcal{I}_{d_0})$)
- **Check** if there exists a solution of IP in $V_{\mathbb{K}}(\mathcal{I}_{d_0})$
  - If **Yes**, **Return** this solution
  - If **No**, **Return** $\emptyset$

Experimental Results – Random instances

$u = n$ $deg = 2$

n	$\#unk.$	q	T_{Gen}	T_{F_5}	T_{F_4/F_5}	T	$q^{n/2}$
8	128	2^{16}	0.3s.	0.1s.	6	0.4s.	2^{64}
15	450	2^{16}	48s.	10s.	23	58s.	2^{120}
17	578	2^{16}	137.2s.	27.9s.	31	195.1s.	2^{136}
20	800	2^{16}	569.1s.	91.5s.	41	660.6s.	2^{160}
15	450	65521	35.5s.	8s.	23	43.5s.	2^{120}
20	800	65521	434.9s.	69.9s.	41	504.8s.	2^{160}
23	1058	65521	1578.6s.	235.9s.		1814s.	2^{184}

N. Courtois, L. Goubin, J. Patarin.
Improved Algorithms for Isomorphism of Polynomials.
EUROCRYPT 1998.

Experimental Results – Random instances

$u = n\ deg = 2$

n	$\#unk.$	q	T_{Gen}	T_{F_5}	T_{F_4/F_5}	T	$q^{n/2}$
8	128	2^{16}	0.3s.	0.1s.	6	0.4s.	2^{64}
15	450	2^{16}	48s.	10s.	23	58s.	2^{120}
17	578	2^{16}	137.2s.	27.9s.	31	195.1s.	2^{136}
20	800	2^{16}	569.1s.	91.5s.	41	660.6s.	2^{160}
15	450	65521	35.5s.	8s.	23	43.5s.	2^{120}
20	800	65521	434.9s.	69.9s.	41	504.8s.	2^{160}
23	1058	65521	1578.6s.	235.9s.		1814s.	2^{184}

We have observed that :

$$d_{\max} = 3.$$

Experimental Results – C* Instances

$u = n$

n	$\#unk.$	q	deg	T_{Gen}	T_{F_5}	T	q^n
5	50	2^{16}	4	0.2s.	0.13s.	0.33s.	2^{80}
6	72	2^{16}	4	0.7s.	1s.	1.7s.	2^{96}
7	98	2^{16}	4	1.5s.	6.1s.	7.6s.	2^{112}
8	128	2^{16}	4	3.8s.	54.3s.	58.1s.	2^{128}
9	162	2^{16}	4	5.4s.	79.8s.	85.2s.	2^{144}
10	200	2^{16}	4	12.9s.	532.3s.	545.2s.	2^{160}

Outline

The HFE scheme

Secret key :

- $(S, U) \in GL_n(\mathbb{K}) \times GL_n(\mathbb{K})$
- $F = \sum_{i,j} \beta_{i,j} X^{q^{\theta_{i,j}} + q^{\theta'_{i,j}}} \in \mathbb{K}'[X]$, with $\mathbb{K}' \supset \mathbb{K}$, $q = \mathrm{Char}(\mathbb{K})$
- $\mathbf{f} = \big(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)\big) \in \mathbb{K}[x_1, \ldots, x_n]^u$

Public key : $(p_1(\mathbf{x}), \ldots, p_n(\mathbf{x})) = (p_1(\mathbf{x} \cdot S), \ldots, p_n(\mathbf{x} \cdot S)) \cdot U$, with $\mathbf{x} = (x_1, \ldots, x_n)$.

J. Patarin.
Hidden Fields Equations (HFE) and Isomorphism of Polynomials (IP): two new families of Asymmetric Algorithms.
EUROCRYPT 1996.

2R and 2R$^-$ Schemes

Secret Key :

- S, U, W dans $GL_n(\mathbb{K})$
- two sets of polynomials ψ et ϕ de $\in \mathbb{K}[x_1, \ldots, x_n]^n$

Public key :

$$\mathbf{h}(\mathbf{x}) = (h_1(\mathbf{x}), \ldots, h_u(\mathbf{x}), \ldots h_n(\mathbf{x})) = \psi\big(\phi(\mathbf{x} \cdot S) \cdot U\big) \cdot W.$$

2R$^-$: we only give $u < n$ polynomials

L. Goubin, J. Patarin.
Asymmetric Cryptography with S-Boxes.
ICICS'97.

Functional Decomposition Problem – (I)

Definition

Let $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$. We shall say that :

$$\left(\mathbf{f} = (f_1, \ldots, f_u), \mathbf{g} = (g_1, \ldots, g_n)\right) \in \mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^n,$$

is a *decomposition* of **h** if :

$$\mathbf{h} = (\mathbf{f} \circ \mathbf{g}) = \left(f_1(g_1, \ldots, g_n), \ldots, f_u(g_1, \ldots, g_n)\right).$$

A decomposition of $(\mathbf{f}, \mathbf{g})$ de **h** is non *trivial* if **f** and **g** are not linear.

Remark

A decomposition $(\mathbf{f}, \mathbf{g})$ of **h** is never unique.
For all $S \in GL_n(\mathbb{K})$, $\mathbf{h}(\mathbf{x}) = \mathbf{f}\left(S \cdot S^{-1}\mathbf{g}(\mathbf{x})\right)$.
$\Rightarrow$ $\left(\mathbf{f}(\mathbf{x} \cdot S), \mathbf{g}(\mathbf{x}) \cdot S^{-1}\right)$ is also a decomposition of **h**.

Functional Decomposition Problem – (II)

FDP

Input : $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$.
Find : a non-trivial decomposition :

- $\mathbf{f} = (f_1, \ldots, f_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$, and
- $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$,

such that :

$$\mathbf{h} = (\mathbf{f} \circ \mathbf{g}) = \big(f_1(g_1, \ldots, g_n), \ldots, f_u(g_1, \ldots, g_n)\big).$$

Functional Decomposition Problem – (II)

FDP(d_f, d_g)

Entrée : $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ and integers $d_f, d_g > 1$

Find : a decomposition :

- $\mathbf{f} = (f_1, \ldots, f_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$
- $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$,

such that :

$$\begin{cases} \mathbf{h} = (\mathbf{f} \circ \mathbf{g}) = \big(f_1(g_1, \ldots, g_n), \ldots, f_u(g_1, \ldots, g_n)\big), \\ \deg(\mathbf{f}) = d_f, \\ \deg(\mathbf{g}) = d_g. \end{cases}$$

Related Works

J. von zur Gathen, J. Gutierrez, R. Rubio
Multivariate Polynomial Decomposition.
Applicable Algebra in Engineering, Communication and Computing, 2004.

D.F. Ye, Z.D. Dai, K.Y. Lam. ($u = n$)
Decomposing Attacks on Asymmetric Cryptography Based on Mapping Compositions.
Journal of Cryptology, 2001.

Preliminary Remarks – (I)

Let :

$$(\mathbf{f} = (f_1, \ldots, f_u), \mathbf{g} = (g_1, \ldots, g_n)) \in \mathbb{K}[\mathbf{x}]^u \times \mathbb{K}[\mathbf{x}]^n,$$

be a non trivial decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$.
The polynomials of **f** can be obtained from **g** by solving a linear system.

For all i, $1 \leq i \leq u$, we have $h_i = f_i(g_1, \ldots, g_n)$

$\Rightarrow$ $\mathcal{O}(u \cdot \mathrm{C}_{n+d_f}^{d_f})$ equations

$\Rightarrow$ $u \cdot \mathrm{C}_{n+d_f}^{d_f}$ unknowns

Preliminary Remarks – (I)

Property

L' *homogenization* of a polynomial $p \in \mathbb{K}[x_1, \ldots, x_n]$ is :

$$p^{\mathrm{H}}(x_0, x_1, \ldots, x_n) = x_0^{\deg(p)} p(x_1/x_0, \ldots, x_n/x_0),$$

x_0 being a new variable. Let :

$$(\mathbf{f} = (f_1, \ldots, f_u), \mathbf{g} = (g_1, \ldots, g_n)) \in \mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^n.$$

We have :

$$(\mathbf{f} \circ \mathbf{g})^{\mathrm{H}} = \mathbf{f}^{\mathrm{H}} \circ \mathbf{g}^{\mathrm{H}},$$

with $\mathbf{f}^{\mathrm{H}} = (x_0^{\deg(\mathbf{f})}, f_1^{\mathrm{H}}, \ldots, f_u^{\mathrm{H}})$ and $\mathbf{g}^{\mathrm{H}} = (x_0^{\deg(\mathbf{g})}, g_1^{\mathrm{H}}, \ldots, g_u^{\mathrm{H}})$.

Summary

Remark

We will focus our attention on FDP(2,2)

- We can suppose w.l.o.g. that the polynomials ($\mathbf{f}$, $\mathbf{g}$) of a decomposition of **h** are homogenous of degree two

Goal

- Find a basis :

$$\mathcal{L}(\mathbf{g}) = \mathrm{Vect}_{\mathbb{K}}(g_1, \ldots, g_n).$$

Intuition – (I)

Let $(\mathbf{f} = (f_1, \ldots, f_u), \mathbf{g} = (g_1, \ldots, g_n)) \in \mathbb{K}[\mathbf{x}]^u \times \mathbb{K}[\mathbf{x}]^n$ be a non-trivial decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$.
For all $i, 1 \leq i \leq u$:

$$h_i = f_i(g_1, \ldots, g_n) = \sum_{1 \leq k,\ell \leq n} f_{k,\ell}^{(i)} \cdot g_k \cdot g_\ell,$$

with $f_i = \sum_{1 \leq k,\ell \leq n} f_{k,\ell}^{(i)} \cdot x_k \cdot x_\ell$. We have then :

$$\frac{\partial h_i}{\partial x_j} = \sum_{1 \leq k,\ell \leq n} f_{k,\ell}^{(i)} \left(\frac{\partial g_k}{\partial x_j} \cdot g_\ell + g_k \cdot \frac{\partial g_\ell}{\partial x_j} \right).$$

Intuition – (II)

Let $(\mathbf{f} = (f_1, \ldots, f_u), \mathbf{g} = (g_1, \ldots, g_n)) \in \mathbb{K}[\mathbf{x}]^u \times \mathbb{K}[\mathbf{x}]^n$ be a non-trivial decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$.
For all $i, 1 \leq i \leq u$:

$$\frac{\partial h_i}{\partial x_j} = \sum_{1 \leq k,\ell \leq n} f_{k,\ell}^{(i)} \left(\frac{\partial g_k}{\partial x_j} \cdot g_\ell + g_k \cdot \frac{\partial g_\ell}{\partial x_j} \right).$$

Thus :

$$\partial \mathcal{I}_h = \left\langle \frac{\partial h_i}{\partial x_j} : 1 \leq i \leq u, 1 \leq j \leq n \right\rangle \subseteq \langle x_k \cdot g_\ell \rangle_{1 \leq k,\ell \leq n}.$$

Description of the Algorithm – (I)

Theorem

Let $(\mathbf{f} = (f_1, \ldots, f_u), \mathbf{g} = (g_1, \ldots, g_n)) \in \mathbb{K}[\mathbf{x}]^u \times \mathbb{K}[\mathbf{x}]^n$, *be a non-trivial decomposition of* $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$, $\mathrm{M}_n(d)$ *the set of monomials of degree* $d \geq 0$ *in* n *variables.*

$$\mathcal{V}_d = \mathrm{Vect}_{\mathbb{K}}\left(m \cdot g_k : m \in \mathrm{M}_n(d+1) \text{ and } 1 \leq k \leq n\right),$$
$$\tilde{\mathcal{V}}_d = \mathrm{Vect}_{\mathbb{K}}\left(m \cdot \frac{\partial h_i}{\partial x_j} : m \in \mathrm{M}_n(d), 1 \leq i \leq u \text{ and } 1 \leq j \leq n\right).$$

If $\dim_{\mathcal{V}_d}(\tilde{\mathcal{V}}_d) = n \cdot |\mathrm{M}_n(d+1)|$, *for some* $d \geq 0$ *:*

$$g_i \in \partial \mathcal{I}_h : x_n^{d+1}, \text{ for all } i, 1 \leq i \leq n.$$

Idea of the Proof – The case $u = n$

$$\frac{\partial h_i}{\partial x_j} = \sum_{1 \leq k,\ell \leq n} f_{k,\ell}^{(i)} \left(\frac{\partial g_k}{\partial x_j} \cdot g_\ell + g_k \cdot \frac{\partial g_\ell}{\partial x_j} \right), \text{for all } i, 1 \leq i \leq u.$$

$$A = \begin{array}{c} \\ \vdots \\ \vdots \\ \frac{\partial h_i}{\partial x_j} \\ \vdots \\ \vdots \end{array} \begin{array}{c} \cdots \quad \cdots \quad x_k \cdot g_\ell \quad \cdots \quad \cdots \\ \left(\begin{array}{c} \cdots \\ \cdots \\ \cdots \\ \cdots \\ \cdots \end{array} \right) \end{array}$$

If A is invertible then :

$$x_n \cdot g_i \in \partial \mathcal{I}_h, \text{for all } i, 1 \leq i \leq n.$$

Idea of the Proof – The case $u < n$

$$m \cdot \frac{\partial h_i}{\partial x_j} = \sum_{1 \le k,\ell \le n} f_{k,\ell}^{(i)} \left(m \cdot \frac{\partial g_k}{\partial x_j} \cdot g_\ell + g_k \cdot \frac{\partial g_\ell}{\partial x_j} \cdot m \right), \text{for all } i, 1 \le i \le u.$$

$$\begin{array}{ccccc} \cdots & \cdots & m' \cdot g_\ell & \cdots & \cdots \end{array}$$

$$A' = \begin{array}{c} \vdots \\ \vdots \\ m \cdot \frac{\partial h_i}{\partial x_j} \\ \vdots \\ \vdots \end{array} \begin{pmatrix} \cdots \\ \cdots \\ \cdots \\ \cdots \\ \cdots \end{pmatrix}$$

If $\mathrm{Rank}(A') = \#\mathrm{columns}(A')$ then :

$$x_n^{d+1} \cdot g_i \in \partial \mathcal{I}_h, \text{for all } i, 1 \le i \le n.$$

Description of the Algorithm – (II)

Corollary

Let $\left(\mathbf{f} = (f_1, \ldots, f_u), \mathbf{g} = (g_1, \ldots, g_n)\right) \in \mathbb{K}[\mathbf{x}]^u \times \mathbb{K}[\mathbf{x}]^n$, be a non-trivial decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$, $\mathrm{M}_n(d)$ the set of monomials of degree $d \geq 0$ in n variables.

Suppose that $\dim_{\mathcal{V}_d}(\tilde{\mathcal{V}}_d) = n \cdot |\mathrm{M}_n(d+1)|$, for some $d \geq 0$. Let G' be DRL-Gröbner basis of $\partial\mathcal{I}_h : x_n^{d+1}$. We have :

$$\mathcal{L}(\mathbf{g}) = \mathrm{Vect}_{\mathbb{K}}(g_1, \ldots, g_n) \subseteq \mathrm{Vect}_{\mathbb{K}}\left(p \in G' : \deg(p) = d_{min}\right).$$

The equality holds if the decomposition is unique.

Description of the Algorithm – (IV)

Let $(\mathbf{f} = (f_1, \ldots, f_u), \mathbf{g} = (g_1, \ldots, g_n)) \in \mathbb{K}[\mathbf{x}]^u \times \mathbb{K}[\mathbf{x}]^n$, be a non-trivial decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$, $\mathrm{M}_n(d)$ the set of monomials of degree $d \geq 0$ in n variables.

- A DRL-Gröbner basis of $\partial\mathcal{I}_h : x_n^{d+1}$ can be computed using standard elimination technique

Complexity Analysis

Property

Let G' be a DRL $(d+3)$-Gröbner basis of $\partial\mathcal{I}_h$. Then :

$$\mathrm{Vect}_{\mathbb{K}}\left(\frac{g'}{x_n^{d+1}} : g' \in G', \text{and } x_n^{d+1} | \mathrm{LM}(g', \prec_{DRL})\right) = \mathcal{L}(\mathbf{g}).$$

If the decomposition is unique.

Generic Complexity [with the F_5 algorithm]

$\mathcal{O}(n^{3(d+3)})$, with $d \approx n/u - 1$

- $\mathcal{O}(n^9)$, for $n = u$ [D.F. Ye, Z.D. Dai, K.Y. Lam, 2001]
- $\mathcal{O}(n^{12})$, for $n/u \approx 2$

Experimental Results

n	b	n_i	r	q	d_{theo}	d_{real}	T	$\sqrt{q^n}$
20	5	4	10	65521	1	1	78.9 s.	$\approx 2^{160}$
20	10	2	10	65521	1	1	78.8 s.	$\approx 2^{160}$
20	2	10	10	65521	1	1	78.7 s.	$\approx 2^{160}$
24	6	4	12	65521	1	1	376.1 s.	$\approx 2^{192}$
30	15	2	15	65521	1	1	2910.5 s.	$\approx 2^{160}$
32	8	4	10	65521	1	1	3287.9 s.	$\approx 2^{256}$
32	8	4	16	65521	1	1	4667.9 s.	$\approx 2^{256}$
36	18	2	15	65521	1	1	13427.4 s.	$\approx 2^{256}$

L. Goubin, J. Patarin.
Asymmetric Cryptography with S-Boxes.
ICICS'97.

Experimental Results

n	b	n_i	r	q	d_{theo}	d_{real}	T	$\sqrt{q^n}$
20	5	4	10	65521	1	1	78.9 s.	$\approx 2^{160}$
20	10	2	10	65521	1	1	78.8 s.	$\approx 2^{160}$
20	2	10	10	65521	1	1	78.7 s.	$\approx 2^{160}$
24	6	4	12	65521	1	1	376.1 s.	$\approx 2^{192}$
30	15	2	15	65521	1	1	2910.5 s.	$\approx 2^{160}$
32	8	4	10	65521	1	1	3287.9 s.	$\approx 2^{256}$
32	8	4	16	65521	1	1	4667.9 s.	$\approx 2^{256}$
36	18	2	15	65521	1	1	13427.4 s.	$\approx 2^{256}$

J.C Faugère, L. P.
An Efficient Algorithm for Decomposing Multivariate Polynomials and its Applications to Cryptography.

Further Algebraic Attacks

- J. H. Silverman, N. P. Smart, F. Vercauteren.
  An Algebraic Approach to NTRU ($q = 2^n$) via Witt Vectors and Overdetermined Systems of Nonlinear Equations.
  SCN 2004.
- G. Bourgeois, J.-C. Faugère.
  Algebraic attack on NTRU with Witt vectors.
  SAGA 2007.
- A. Bauer, A. Joux.
  Toward a Rigorous Variation of Coppersmith's Algorithm on Three Variables.
  Eurocrypt 2007.

Further Reading (In preparation ...)

- Invited Editors : D. Augot, J.-C Faugère, L. P.
  Gröbner Bases Techniques in Cryptography and Coding Theory
  Special Issue – Journal of Symbolic Computation.
- Invited Editors : T. Mora, M. Sala, C. Traverso, L. P., M. Sakata.
  Gröbner Bases in Coding Theory and Cryptography.
  RISC book series (Springer, Heidelberg)
- Invited Editors : J.-C Faugère, F. Rouiller.
  Efficient Computation of Gröbner Bases.
  Special Issue – Journal of Symbolic Computation.