Gröbner Bases in Public-Key Cryptography

Ludovic Perret

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

ECRYPT PhD SUMMER SCHOOL
Emerging Topics in Cryptographic Design and Cryptanalysis

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 an algebraic set of equations
- Try to solve this system

  $\Rightarrow$ Gröbner bases

Why Using Gröbner Bases ?

- Based on an elegant and rich mathematical theory
  $\Rightarrow$ Buchberger's talk
- Most efficient method for solving algebraic systems
- Efficient implementations available
  - Buchberger's algorithm (Singular, Gb, ...)
  - F_4 algorithm (Magma, Maple 10, Fgb, ...)

Efficient Algebraic Cryptanalysis ?

- Convert a cryptosystem into an algebraic set of equations

  a particular attention to the way of constructing the system

  exploit all the properties of the cryptosystem

- Try to solve the simplified system

Efficient Algebraic Cryptanalysis ?

- Convert a cryptosystem into an algebraic set of equations

  a particular attention to the way of constructing the system

  exploit all the properties of the cryptosystem

- Try to solve the simplified system

  $\Rightarrow$ Minimize the number of variables/degree

  $\Rightarrow$ Maximize the number of equations

Efficient Algebraic Cryptanalysis ?

- Convert a cryptosystem into an algebraic set of equations
  a particular attention to the way of constructing the system
  exploit all the properties of the cryptosystem
- Simplify the system
- Try to solve the simplified system
  $\Rightarrow$ Minimize the number of variables/degree
  $\Rightarrow$ Maximize the number of equations

Algebraic Cryptanalysis in Practice

- Block Ciphers ($\Rightarrow$ Cid's talk)
- Stream Ciphers ($\Rightarrow$Johansson/Canteaut 's talk & Cid's talk)

$\vdots$

Outline

The HFE scheme

[J. Patarin, Eurocrypt 1996]

Secret key :

- $(S, U) \in GL_n(\mathbb{K}) \times GL_n(\mathbb{K})$
- $A = \sum_{i,j} \beta_{i,j} X^{q^{\theta_{i,j}} + q^{\theta'_{i,j}}} \in \mathbb{K}'[X]$, with $\mathbb{K}' \supset \mathbb{K}$, $q = Char(\mathbb{K})$
- $\mathbf{a} = \big(a_1(x_1, \ldots, x_n), \ldots, a_n(x_1, \ldots, x_n)\big) \in \mathbb{K}[x_1, \ldots, x_n]^u$

Public key :

$$\big(b_1(\mathbf{x}), \ldots, b_n(\mathbf{x})\big) = \big(a_1(\mathbf{x}S), \ldots, a_n(\mathbf{x}S)\big)\, U,$$

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

Encryption : To enc. $\mathbf{m} \in \mathbb{K}^n$, $\mathbf{c} = \big(b_1(\mathbf{m}), \ldots, b_n(\mathbf{m})\big)$.

Signature : To sig. $\mathbf{m} \in \mathbb{K}^n$, find $\mathbf{s} \in \mathbb{K}^n$ s.t. $\mathbf{b}(\mathbf{s}) = \mathbf{m}$.

Message Recovery Attack – (I)

Given $\mathbf{c} = \left(b_1(\mathbf{m}), \ldots, b_n(\mathbf{m})\right) \in \mathbb{K}^n$. Find $\mathbf{z} \in \mathbb{K}^n$, such that :

$$b_1(\mathbf{z}) - c_1 = 0, \ldots, b_n(\mathbf{z}) - c_n = 0.$$

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 ...

Complexity of F_5 : $2^{O(log(n)^2)}$.

- J.-C. Faugère, A. Joux.
  Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases.
  CRYPTO 2003.
- L. Granboulan, A. Joux, J. Stern.
  Inverting HFE is Quasipolynomial.
  CRYPTO 2006.

Outline

"Key Recovery Attack"

2PLE

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. :

$$\left(b_1(\mathbf{x}), \ldots, b_n(\mathbf{x})\right) = \left(a_1(\mathbf{x}S), \ldots, a_n(\mathbf{x}S)\right) U,$$

denoted by $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x}S)U$, 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.

A Basic Problem – (I)

- HFE and related schemes (C^*, SFLASH, ...)
  - $A = X^{1+q^\theta} \in \mathbb{K}'[X]$, with $\mathbb{K}' \supset \mathbb{K}$, and $q = Char(\mathbb{K})$
- signature/authentication schemes

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

- Traitor Tracing schemes

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

A Basic Problem – (II)

Code Equivalence (CE)

Given : two matrices G_1, and $G_2 \in \mathcal{M}_{k,n}(\mathbb{F}_q)$.
Find : – if any – $S \in GL_k(\mathbb{F}_q)$, and a permutation $\sigma \in \mathcal{S}_n$, s.t. :

$$G_2 = S G_1 P_\sigma,$$

where :

$$\begin{cases} (P_\sigma)_{i,j} = 1, \text{ if } \sigma(i) = j, \text{ and} \\ (P_\sigma)_{i,j} = 0, \text{ otherwise.} \end{cases}$$

A Basic Problem – cont'd

McEliece's Cryptosystem (1978)

Secret key : $S \in GL_k(\mathbb{F}_2)$, a permutation σ on $\{1, \ldots, n\}$.
Public data : $G \in \mathcal{M}_{k,n}(\mathbb{F}_2)$
Public key :

$$G' = SGP_\sigma,$$

where :

$$\begin{cases} (P_\sigma)_{i,j} = 1, \text{ if } \sigma(i) = j, \text{ and} \\ (P_\sigma)_{i,j} = 0, \text{ otherwise.} \end{cases}$$

Encryption : To encrypt $\underline{m} \in \mathbb{F}_2^k$, compute:

$$\underline{c} = \underline{m}G' + \underline{e},$$

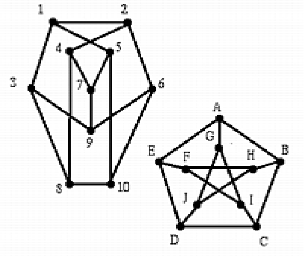
with $\underline{e} \in \mathbb{F}_2^n$, s.t. $w_H(e) = t$.

A Basic Problem – cont'd

Graph Isomorphism Problem

Given : $\mathcal{G}_1 = (V_1, E_1), \mathcal{G}_2 = (V_2, E_2)$
Question : Find – if any – a bijection $p : V_1 \to V_2$, such that:

$$(i,j) \in E_1 \text{ if, and only if,} \big(p(i), p(j)\big) \in E_2.$$



Hard Problems ?

N. Sendrier.
Finding the permutation between equivalent codes: the Support Splitting Algorithm.
IEEE Transactions on Information Theory, July 2000.

L. Babai.
Automorphism groups, isomorphism, reconstruction.
Handbook of combinatorics.

Outline

Basic Idea – (I)

Fact

Suppose that $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x}S)U$, *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. :*

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

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

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

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 :*

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

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

$$(\phi_1(S), \phi_2(U^{-1})) \in V(\mathcal{I}),$$

with :

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

A Structural Property

Lemma

Let d be a positive integer, and $\mathcal{I}_d \subset \mathbb{F}_q[\mathbf{y}, \mathbf{z}]$ be the ideal generated by the polynomials $p\alpha_i$ of maximal total degree smaller than d. Let also $V(\mathcal{I}_d)$ be the variety associated to $\mathcal{I}_d$. If $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x}S)U$, for some $(S, U) \in GL_n(\mathbb{K}) \times GL_u(\mathbb{K})$, then :

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

with:

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

The 2PLE 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. $\mathbf{b}(\mathbf{x}) = \mathbf{a}(\mathbf{x}S)U$

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

- **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** $V(\mathcal{I}_{d_0})$
- **Find** a solution of 2PLE among the elements of $V(\mathcal{I}_{d_0})$
- **Return** this solution

Summary

We solve algebraic systems of :

- $O(u \cdot n^{d_0})$ equations of degree at most d_0
  - $d_0 = 2$ in practice
- $n^2 + u^2$ unknowns

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 – 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

[J. Patarin, Eurocrypt 1996]

Secret key :

- $(S, U) \in GL_n(\mathbb{K}) \times GL_n(\mathbb{K})$
- $A = \sum_{i,j} \beta_{i,j} X^{q^{\theta_{i,j}} + q^{\theta'_{i,j}}} \in \mathbb{K}'[X]$, with $\mathbb{K}' \supset \mathbb{K}$, $q = Char(\mathbb{K})$
- $\mathbf{a} = \big(a_1(x_1, \ldots, x_n), \ldots, a_n(x_1, \ldots, x_n)\big) \in \mathbb{K}[x_1, \ldots, x_n]^u$

Public key :

$$\big(b_1(\mathbf{x}), \ldots, b_n(\mathbf{x})\big) = \big(a_1(\mathbf{x}S), \ldots, a_n(\mathbf{x}S)\big)\, U,$$

with $\mathbf{x} = (x_1, \ldots, x_n)$.
Encryption : To enc. $\mathbf{m} \in \mathbb{K}^n$, $\mathbf{c} = \big(b_1(\mathbf{m}), \ldots, b_n(\mathbf{m})\big)$.
Signature : To sig. $\mathbf{m} \in \mathbb{K}^n$, find $\mathbf{s} \in \mathbb{K}^n$ s.t. $\mathbf{b}(\mathbf{s}) = \mathbf{m}$.

2R/2R$^-$ schemes

SK :

- Three affine bijections $r, s, t : \mathbb{K}^n \rightarrow \mathbb{K}^n$
- Two applications $\psi, \phi : \mathbb{K}^n \rightarrow \mathbb{K}^n$

PK : $h_1, \ldots, h_u, \ldots, h_n \in \mathbb{K}[x_1, \ldots, x_n]$ describing :

$$\mathbf{h} = \underbrace{t \circ \psi \circ s}_{\mathbf{f}} \circ \underbrace{\phi \circ r}_{\mathbf{g}}, \mathbb{K}^n \rightarrow \mathbb{K}^n.$$

2R$^-$ schemes : some polynomials of the PK are removed

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

Functional Decomposition Problem

FDP

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

Find :

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

such that :

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

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.

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.

E. Biham.
Cryptanalysis of Patarin's 2-Round Public Key System with S-Boxes (2R).
CRYPTO 2000.

Outline

Preliminary Remarks – (I)

FDP

Find $\mathbf{f} = (f_1, \ldots, f_u) : \mathbb{K}^n \to \mathbb{K}^u, \mathbf{g} = (g_1, \ldots, g_n) : \mathbb{K}^n \to \mathbb{K}^n$, s. t.

$$\mathbf{h} = (h_1, \ldots, h_u) = \big(f_1(g_1, \ldots, g_n), \ldots, f_u(g_1, \ldots, g_n)\big).$$

[D.F. Ye, Z.D. Dai, K.Y. Lam, 2001]

- $h_1, \ldots, h_u$ are polynomials of degree 4
- Restrict our attention to homogeneous instances
  - $f_1, \ldots, f_u, g_1, \ldots, g_n$ are homogeneous quadratic poly.

Preliminary Remarks – (II)

FDP

Find $\mathbf{f} = (f_1, \ldots, f_u) : \mathbb{K}^n \to \mathbb{K}^u$, $\mathbf{g} = (g_1, \ldots, g_n) : \mathbb{K}^n \to \mathbb{K}^n$, s. t.

$$\mathbf{h} = (h_1, \ldots, h_u) = \big(f_1(g_1, \ldots, g_n), \ldots, f_u(g_1, \ldots, g_n)\big).$$

- The f_is can be deduced from the g_is.
- Let $L : \mathbb{K}^n \to \mathbb{K}^n$ be a bijective linear mapping, then :

$$h = (f \circ L^{-1}) \circ (L \circ g).$$

Description of the Algorithm – (I)

FDP

Find $\mathbf{f} = (f_1, \ldots, f_u) : \mathbb{K}^n \rightarrow \mathbb{K}^u$, $\mathbf{g} = (g_1, \ldots, g_n) : \mathbb{K}^n \rightarrow \mathbb{K}^n$, s. t.

$$\mathbf{h} = (h_1, \ldots, h_u) = \big(f_1(g_1, \ldots, g_n), \ldots, f_u(g_1, \ldots, g_n)\big).$$

Goal

- Find a basis of $\mathcal{L}(g) = \mathrm{Vect}(g_1, \ldots, g_n)$.

Property

Let $\partial\mathcal{I}_h = \left\langle \frac{\partial h_i}{\partial x_j} : 1 \leq i \leq u, 1 \leq j \leq n \right\rangle$, then for all $i, 1 \leq i \leq n$:

$$x_n^{d+1} \cdot g_i \in \partial\mathcal{I}_h, \text{ for some } d \geq 0.$$

Description of the Algorithm – (II)

Property

A (red.) DRL Gröbner basis of an ideal $\mathcal{I}$ contains a basis of

$$\left\{ Q \in \mathcal{I} : \deg(Q) = \min_{Q \in \mathcal{I}}\left(\deg(Q)\right) \right\}.$$

Lemma

Let G' be a reduced DRL Gröbner basis of $\partial\mathcal{I}_h$. Then :

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

provided that the decomposition is "unique".

Complexity Analysis

Property

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

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

Conjectured Complexity [with the F_5 algorithm]

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

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

Remark

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

Further Algebraic Attack

- 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.

Next Challenge

(Algebraic) Cryptanalysis of :

- HFE–
- UOV

Algebraic Cryptanalysis of NTRU

Initial Problem

- Algebraic System over $\mathbb{Z}_{2^n}$

Ring of Witt Vectors $(\mathrm{W}_m(\mathbb{F}_2),+,\cdot)$

$\mathrm{W}_m(\mathbb{F}_2) : [a_0, \ldots, a_{m-1}] \in \mathbb{F}_2^m$ $(\mapsto \sum_{i=0}^{m-1} a_i 2^i \in \mathbb{Z}_{2^m})$
Let $a = [a_0, \ldots, a_{m-1}]$, $b = [b_0, \cdots, b_{m-1}]$

- $a + b = [S_0(a,b), \ldots, S_{m-1}(a,b)]$
- $a \cdot b = [P_0(a,b), \cdots, P_{m-1}(a,b)]$

where:
$S_0, \ldots, S_{m-1}, P_0, \ldots, P_{m-1} \in \mathbb{F}_2[x_0, \ldots, x_{m-1}, y_0, \ldots, y_{m-1}]$.

- $S_0(a,b) = a_0 + b_0$, $P_0(a,b) = a_0 b_0$
- $S_1(a,b) = a_0 b_0 + a_1 + b_1$, $P_1(a,b) = a_0 b_1 + b_0 a_1$

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, Coding, 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