High Order Derivatives and Decomposition of Multivariate Polynomials

Jean-Charles Faugère, and Ludovic Perret

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

ISSAC 2009

Outline

1 Functional Decomposition
- Symbolic Computation & Cryptography

2 New Algorithm for FDP

Outline

1 Functional Decomposition
- Symbolic Computation & Cryptography

2 New Algorithm for FDP

Functional Decomposition Problem – 1/2

Definition

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

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

is a *decomposition* of $\mathbf{h}$ if:

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

Remark

A decomposition $(\mathbf{f}, \mathbf{g})$ of $\mathbf{h}$ is never unique, $\forall S \in GL_n(\mathbb{K})$:

$$\mathbf{h}(\mathbf{x}) = \mathbf{f}\big(\mathbf{g}(\mathbf{x}) \cdot S^{-1} S\big).$$

$\Rightarrow \big(\mathbf{f}(\mathbf{x} \cdot S), \mathbf{g}(\mathbf{x}) \cdot S^{-1}\big)$ is also a decomposition of $\mathbf{h}$.

Functional Decomposition Problem – 2/2

FDP(d_f, d_g)

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

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

Remark

- $\mathbf{f} = (f_1, \ldots, f_u)$ are supposed to be of the same degree d_f
- $\mathbf{g} = (g_1, \ldots, g_n)$ are supposed to be of the same degree d_g

Related Works

J. von zur Gathen.

“Functional decomposition of polynomials: the tame case."

“Functional decomposition of polynomials: the wild case".

J. Symb. Comput., 1990.

J. von zur Gathen.

“Counting decomposable univariate polynomials". ISSAC’09.

J. von zur Gathen, J. Gutierrez, R. Rubio.

“Multivariate Polynomial Decomposition." AAECC, 2004.

E.-W. Chionh, X.-S. Gao, L.-Y. Shen.

Inherently Improper Surface Parametric Supports. Computer Aided Geometric Design, 2006.

S. M. Watt.

Functional Decomposition of Symbolic Polynomials. ICCSA’08.

Outline

1 Functional Decomposition
- Symbolic Computation & Cryptography

2 New Algorithm for FDP

Multivariate Cryptograhy : 2R$^-$ Schemes

Secret key

- L_0, L_1, L_2 in $GL_n(\mathbb{K})$
- two sets of polynomials ψ and ϕ of $\mathbb{K}[x_1, \ldots, x_n]^n$

Public key

$$\mathbf{h}(\mathbf{x}) = (h_1(\mathbf{x}), \ldots, h_u(\mathbf{x})) = \psi\big(\phi(\mathbf{x} \cdot L_0) \cdot L_1\big) \cdot L_2.$$


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


J.-C. Faugère.
Symbolic Computation and Cryptography.
Tutorial, ISSAC 2009.

Related Works

- D.F. Ye, Z.D. Dai, K.Y. Lam. (FDP(2,2),$u = n$)
  Decomposing Attacks on Asymmetric Cryptography Based on Mapping Compositions. Journal of Cryptology, 2001.
- J.-C. Faugère, L. Perret. (FDP(2,2), $u < n$)
  Cryptanalysis of 2R$^-$ schemes. CRYPTO 2006.
- J.-C. Faugère, L. Perret. (FDP(d_f, d_g))
  An Efficient Algorithm for Decomposing Multivariate Polynomials and its Applications to Cryptography. Special Issue of J. Symb. Comput. on “Gröbner Bases Techniques in Coding Theory and Cryptography".

Old algorithm

FDP(d_f, d_g) –> (FDP($d_f - 1, d_g$),FDP($d_f - 2, d_g$),..., FDP($2, d_g$))

Outline

1 Functional Decomposition
- Symbolic Computation & Cryptography

2 New Algorithm for FDP

Preliminary Remarks – 1/2

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 decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$.

For all $i, 1 \leq i \leq u$, we have:

$$h_i = f_i(g_1, \ldots, g_n).$$

$\Rightarrow$ $\mathbf{f}$ can be obtained from $\mathbf{g}$ by solving a linear system.

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

Preliminary Remarks – 2/2

- We suppose that the polynomials $(\mathbf{f}, \mathbf{g})$ of a decomposition of $\mathbf{h}$ are homogenous of the same degrees d_f and d_g.

Remark

A decomposition $(\mathbf{f}, \mathbf{g})$ of $\mathbf{h}$ is never unique, $\forall S \in GL_n(\mathbb{K})$:

$$\mathbf{h}(\mathbf{x}) = \mathbf{f}\big(\mathbf{g}(\mathbf{x}) \cdot S^{-1} S\big).$$

$\Rightarrow \big(\mathbf{f}(\mathbf{x} \cdot S), \mathbf{g}(\mathbf{x}) \cdot S^{-1}\big)$ is also a decomposition of $\mathbf{h}$.

Goal

- Find a basis:

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

Intuition – 1/2

Example : we consider FDP(3,2).

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 $(3,2)$ decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$. For all $i, 1 \leq i \leq u$:

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

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

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

Thus:

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

Old idea

Intuition – 1/2

Example : we consider FDP(3,2).

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 $(3,2)$ decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$. For all $i, 1 \leq i \leq u$:

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

$$\frac{\partial^2 h_i}{\partial x_j \partial x_r} = \sum_{1 \leq k,\ell,m \leq n} f_{k,\ell,m}^{(i)} \left(\frac{\partial g_k}{\partial x_j}\frac{\partial g_\ell}{\partial x_r} g_m + g_k \frac{\partial g_\ell}{\partial x_j}\frac{\partial g_m}{\partial x_r} + \frac{\partial g_k}{\partial x_j}\frac{\partial g_m}{\partial x_r} g_\ell + \right.$$

$$\frac{\partial g_k}{\partial x_r}\frac{\partial g_\ell}{\partial x_j} g_m + g_k \frac{\partial g_\ell}{\partial x_r}\frac{\partial g_m}{\partial x_j} + \frac{\partial g_k}{\partial x_r}\frac{\partial g_m}{\partial x_j} g_\ell$$

$$\left. \frac{\partial^2 g_k}{\partial x_j \partial x_r} g_\ell g_m + \frac{\partial^2 g_\ell}{\partial x_j \partial x_r} g_m g_k + \frac{\partial^2 g_m}{\partial x_j \partial x_r} g_k g_\ell \right).$$

New approach

Intuition – 2/2

Example : we consider FDP(3,2).

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 $(3,2)$ decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$.

$$\frac{\partial^2 h_i}{\partial x_j \partial x_r} = \sum_{1 \le k,\ell,m \le n} f^{(i)}_{k,\ell,m} \left(\frac{\partial g_k}{\partial x_j}\frac{\partial g_\ell}{\partial x_r} g_m + g_k \frac{\partial g_\ell}{\partial x_j}\frac{\partial g_m}{\partial x_r} + \frac{\partial g_k}{\partial x_j}\frac{\partial g_m}{\partial x_r} g_\ell + \right.$$
$$\frac{\partial g_k}{\partial x_r}\frac{\partial g_\ell}{\partial x_j} g_m + g_k \frac{\partial g_\ell}{\partial x_r}\frac{\partial g_m}{\partial x_j} + \frac{\partial g_k}{\partial x_r}\frac{\partial g_m}{\partial x_j} g_\ell$$
$$\left. \frac{\partial^2 g_k}{\partial x_j \partial x_r} g_\ell g_m + \frac{\partial^2 g_\ell}{\partial x_j \partial x_r} g_m g_k + \frac{\partial^2 g_m}{\partial x_j \partial x_r} g_k g_\ell \right).$$

Thus:

$$\partial^2 \mathcal{I}_h = \left\langle \frac{\partial^2 h_i}{\partial x_j \partial x_r} \mid 1 \le i \le u, 1 \le j, r \le n \right\rangle \subseteq \langle x_k \cdot x_\ell \cdot g_m \rangle_{1 \le k,\ell,m \le n}.$$

$u = n$

$$\frac{\partial^2 h_i}{\partial x_j \partial x_r} = \sum_{1 \le k,\ell,m \le n} f^{(i)}_{k,\ell,m} \left(\frac{\partial g_k}{\partial x_j}\frac{\partial g_\ell}{\partial x_r} g_m + g_k \frac{\partial g_\ell}{\partial x_j}\frac{\partial g_m}{\partial x_r} + \frac{\partial g_k}{\partial x_j}\frac{\partial g_m}{\partial x_r} g_\ell + \right.$$

$$\frac{\partial g_k}{\partial x_r}\frac{\partial g_\ell}{\partial x_j} g_m + g_k \frac{\partial g_\ell}{\partial x_r}\frac{\partial g_m}{\partial x_j} + \frac{\partial g_k}{\partial x_r}\frac{\partial g_m}{\partial x_j} g_\ell$$

$$\left. \frac{\partial^2 g_k}{\partial x_j \partial x_r} g_\ell g_m + \frac{\partial^2 g_\ell}{\partial x_j \partial x_r} g_m g_k + \frac{\partial^2 g_m}{\partial x_j \partial x_r} g_k g_\ell \right).$$

$$A = \begin{array}{c} \\ \vdots \\ \frac{\partial^2 h_i}{\partial x_j \partial x_r} \\ \vdots \\ \vdots \end{array} \begin{pmatrix} \cdots & \cdots & x_k \cdot x_m \cdot g_\ell & \cdots & \cdots \\ & & \cdots & & \\ & & \cdots & & \\ & & & & \\ & & \cdots & & \\ & & \cdots & & \end{pmatrix}$$

If $\mathrm{Rank}(A) = n^3$, then $x_n^2 \cdot g_i \in \partial \mathcal{I}_h^2$, for all $i, 1 \le i \le n$.

$u < n$

m be a monomial of degree δ.

$$m \cdot \frac{\partial^2 h_i}{\partial x_j \partial x_r} = \sum_{1 \le k,\ell,m \le n} m \cdot f^{(i)}_{k,\ell,m} \left(\frac{\partial g_k}{\partial x_j}\frac{\partial g_\ell}{\partial x_r} g_m + g_k \frac{\partial g_\ell}{\partial x_j}\frac{\partial g_m}{\partial x_r} + \frac{\partial g_k}{\partial x_j}\frac{\partial g_m}{\partial x_r} g_\ell + \right.$$
$$\frac{\partial g_k}{\partial x_r}\frac{\partial g_\ell}{\partial x_j} g_m + g_k \frac{\partial g_\ell}{\partial x_r}\frac{\partial g_m}{\partial x_j} + \frac{\partial g_k}{\partial x_r}\frac{\partial g_m}{\partial x_j} g_\ell$$
$$\left. \frac{\partial^2 g_k}{\partial x_j \partial x_r} g_\ell g_m + \frac{\partial^2 g_\ell}{\partial x_j \partial x_r} g_m g_k + \frac{\partial^2 g_m}{\partial x_j \partial x_r} g_k g_\ell \right).$$

$$A'_\delta = \begin{array}{c} \\ \vdots \\ m \cdot \frac{\partial^2 h_i}{\partial x_j \partial x_r} \\ \vdots \end{array} \begin{array}{c} \cdots \quad \cdots \quad m' \cdot g_\ell \quad \cdots \quad \cdots \\ \begin{pmatrix} & \cdots & \\ & \cdots & \\ & \cdots & \end{pmatrix} \end{array}$$

If $\mathrm{Rank}(A'_\delta) = \#\mathrm{columns}(A'_\delta)$, $x_n^{\delta+2} \cdot g_i \in \partial\mathcal{I}_h^2$, for all $i, 1 \le i \le n$.

Intuition – FDP$(d_f, 2)$

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 $(d_f, 2)$ decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$. We can write:

$$\frac{\partial^{(d_f-1)} h_i}{\partial^{j_1} x_{i_1} \cdots \partial^{j_r} x_{i_r}} = \sum_{1 \leq k \leq n} p_k(x_1, \ldots, x_n) g_k,$$

with p_k homogeneous poly. of degree $d_f - 1$.

We now consider:

$$\partial^{(d_f-1)} \mathcal{I}_h = \left\langle \frac{\partial^{(d_f-1)} h_i}{\partial^{j_1} x_{i_1} \cdots \partial^{j_r} x_{i_r}} \right\rangle.$$

Key Idea of the Algorithm – 1/2

Theorem

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* $(d_f, 2)$ *decomposition of* $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$ *, and:*

$$A'_\delta = \begin{array}{c} \\ \\ m \cdot \frac{\partial^{(d_f-1)} h_i}{\partial^{j_1} x_{i_1} \cdots \partial^{j_r} x_{i_r}} \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} \cdots & \cdots & m' \cdot g_\ell & \cdots & \cdots \end{array} \\ \begin{pmatrix} & \cdots & \\ & \cdots & \\ & & \\ & \cdots & \end{pmatrix} \end{array}$$

If $\mathrm{Rank}(A'_\delta) = \#\mathrm{columns}(A'_\delta)$*, for some* $\delta \geq 0$*, then:*

$$x_n^{\delta+d_f-1} \cdot g_i \in \partial^{(d_f-1)} \mathcal{I}_h, \text{ for all } i, 1 \leq i \leq n.$$

Key Idea of the Algorithm – 1/2

Theorem

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* $(d_f, 2)$ *decomposition of* $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$ *If* $\mathrm{Rank}(A'_\delta) = \#\mathrm{columns}(A'_\delta)$, *for some* $\delta \geq 0$, *then:*

$$x_n^{\delta+d_f-1} \cdot g_i \in \partial^{(d_f-1)}\mathcal{I}_h, \text{ for all } i, 1 \leq i \leq n.$$

Remark

"Generic" bound can be obtained on δ.

- For "small values" of u and n, such δ never exists.
  - In FDP(2,2), we must have $n \geq 6$ (if $u = n$).

Key Idea of the Algorithm – 2/2

$$\partial^{(d_f-1)}\mathcal{I}_h : x_n^{\delta+d_f-1} = \left\{ p \in \mathbb{K}[x_1, \ldots, x_n] \mid p \cdot x_n^{\delta+d_f-1} \in \partial\mathcal{I}_h^{(d_f-1)} \right\}.$$

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 $(d_f, 2)$ decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$.
If $\mathrm{Rank}(A'_\delta) = \#\mathrm{columns}(A'_\delta)$, for some $\delta \geq 0$:

$$\langle g_1, \ldots, g_n \rangle \subset \partial\mathcal{I}_h : x_n^{\delta+d_f-1}.$$

Let G' be DRL-Gröbner basis of $\partial\mathcal{I}_h : x_n^{\delta+d_f-1}$, then:

$$\mathcal{L}(\mathbf{g}) = \mathrm{Vect}_{\mathbb{K}}(g_1, \ldots, g_n) \subseteq \mathrm{Vect}_{\mathbb{K}}\big(p \in G' \mid \deg(p) = 2\big).$$

The equality is not valid if the decomposition is not “unique".

(Pseudo) algorithm

FDP($d_f \geq 2, 2$)

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 $(d_f, 2)$ decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$.

- Compute a DRL-Gröbner basis G' of $\partial^{(d_f-1)}\mathcal{I}_h : x_n^{\delta+d_f-1}$, for some $\delta \geq 0$.
- Output $\left\{ p \in G' \mid \deg(p) = 2 \right\}$.

Old approach

FDP(d_f, d_g) –> (FDP($d_f - 1, d_g$),FDP($d_f - 2, d_g$),. . . , FDP($2, d_g$))

Advantages of the new approach

- Only one (cheaper) Gröbner basis computation

Experimental Results – FDP(3,2)

u	n	d_f	δ_{exp}	δ_{theo}	$x_n^{d_f-1+\delta_{\text{exp}}}$	T_{New}	T_{Old}
6	6	3	0	0	x_n^2	0.01 s.	0.12 s.
7	7	3	0	0	x_n^2	0.02 s.	0.33 s.
8	8	3	0	0	x_n^2	0.07 s.	0.86 s.
15	15	3	0	0	x_n^2	10.7 s.	311.4 s.
16	16	3	0	0	x_n^2	19.2 s.	577.9 s.
17	17	3	0	0	x_n^2	33.6 s.	1110.9 s.
4	7	3	1	1	x_n^3	0.04 s.	0.21 s.
4	8	3	1	1	x_n^3	0.1 s.	0.51 s.
9	18	3	1	1	x_n^3	1349.3 s.	
10	20	3	1	1	x_n^3	9688.9 s.	
7	7	4	0	0	x_n^3	0.16 s.	
8	8	4	0	0	x_n^3	0.65 s.	
9	9	4	0	0	x_n^3	0.93 s.	
10	10	4	0	0	x_n^3	7.5 s.	

Conclusion

- Method can be generalized for $d_g \geq 2$ and for “mixed" instances.
- “Generic" bound can be obtained on δ.
  - leads to a complexity bound.
- A rather general algorithm for decomposing multivariate polynomials, but
  - Open problem(s) related to the definition of the FDP
    - Multivariate equivalent of Ritt’s Second Theorem ?
- Application(s) in cryptography (stream ciphers) ?

Symbolic Computation $\mapsto$ Cryptography $\mapsto$ Symbolic Computation

Conclusion – con't

Definition

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 decomposition of $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[\mathbf{x}]^u$. This decomposition is non trivial if $\mathbb{K}[h_1, \ldots, h_u] \subset \mathbb{K}[g_1, \ldots, g_n] \subset \mathbb{K}[x_1, \ldots, x_n]$.

The FDP problem is then equivalent to find a proper intermediate $\mathbb{K}$-algebra between $\mathbb{K}[h_1, \ldots, h_u]$ and $\mathbb{K}[x_1, \ldots, x_n]$.

Definition

We shall say that $\left(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\right)$ is a generic decomposition of h if the polynomials of f and g are generics.

For a generic decomposition, we conjecture that trivial cases occur only when $d_f = 1$ or $d_g = 1$.