An Efficient Algorithm for Decomposing Multivariate Polynomials and its Applications to Cryptography

Jean-Charles Faugère and Ludovic Perret

SALSA *Project*
INRIA, Centre Paris-Rocquencourt
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
104, avenue du Président Kennedy
75016 Paris, France

Abstract

In this paper, we present an efficient and general algorithm for decomposing multivariate polynomials of the same arbitrary degree. This problem, also known as the *Functional Decomposition Problem* (FDP) (31), is classical in computer algebra. It is the first general method addressing the decomposition of multivariate polynomials (any degree, any number of polynomials). As a byproduct, our approach can be also used to recover an ideal $\mathcal{I}$ from its k-th power $\mathcal{I}^k$. The complexity of the algorithm depends on the ratio between the number of variables (n) and the number of polynomials (u). For example, polynomials of degree four can be decomposed in $\mathcal{O}(n^{12})$, when this ratio is smaller than $\frac{1}{2}$. This works was initially motivated by a cryptographic application, namely the cryptanalysis of $2R^-$ schemes (16; 17). From a cryptographic point of view, the new algorithm is so efficient that the principle of two-round schemes, including $2R^-$ schemes, becomes useless. Besides, we believe that our algorithm is of independent interest.

Key words: Multivariate Polynomials Decomposition, Gröbner bases, Cryptography.

1. Introduction

In this paper, we describe an efficient method for solving the so-called *Functional Decomposition Problem* (FDP) (31). This problem is as follows : given a set of u polynomials $h = (h_1, \ldots, h_u)$ over a polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ ($\mathbb{K}$ denoting an arbitrary

⋆

Email address: Jean-Charles.Faugere@inria.fr, ludovic.perret@lip6.fr (Jean-Charles Faugère and Ludovic Perret).

field) our algorithm permits to recover – if any – $f = (f_1, \ldots, f_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ and $g = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$ whose composition equals to h, i.e.

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

This works was initially motivated by a cryptographic application, namely the cryptanalysis of $2R^-$ schemes (16; 17). Besides, FDP is a classical problem in computer algebra : for instance in the univariate case, the decomposition is a standard functionality proposed in some computer algebra systems (for example, we can mention the function `compoly` of Maple [1]).

1.1. Previous Works

The univariate decomposition was 25 years ago considered as computationally hard. A cryptographic protocol has been even based on this problem (5). Nowadays, nobody will be really confident on such system. Indeed, there is now a vast literature proposing efficient algorithms for decomposing univariate polynomials e.g. (29; 30).

In (18), von zur Gathen, Gutierrez and Rubio have studied several restrictions of FDP, namely the *uni-multivariate*, *multi-univariate* and *single-variable* decompositions. From an algorithmic point of view, they proposed an efficient method for decomposing multi-univariate polynomials. From a theoretical point of view, they proved the uniqueness (in an appropriate sense) of the uni-multivariate, multi-univariate decompositions and the finiteness of uni-multivariate, multi-univariate and single-variable decompositions. We will also quote Dickerson who has proved that FDP is NP-Hard (10; 11). Note that this fact is not in contradiction with the result presented in this paper since our method is really efficient only when the ratio $\frac{n}{u}$ is not too small.

Ye, Dai and Lam (14) have proposed an efficient algorithm for decomposing a set of n polynomials of degree four into two sets of n quadratic polynomials. Their algorithm essentially used linear algebra techniques, but is limited to the special case $u = n$.

In (14), the two authors of this paper have extended the algorithm presented (31; 32) for decomposing instances of FDP for which the number of polynomials is smaller or equal than the number of variables ($u \leq n$). To do so, we have used a fundamental tool of commutative algebra, namely Gröbner bases (6; 7). However, this algorithm only permitted to decompose polynomials of degree four (composition of quadratic polynomials).

We will present here a extension of the technique introduced in (14) allowing to decompose polynomials of *arbitrary degree*. To our knowledge, this is the first general algorithm addressing the multivariate case. As a byproduct, our approach can be also used to recover an ideal $\mathcal{I}$ from its k-th power $\mathcal{I}^k$. The complexity of our algorithm will depend of the degree of the input polynomials, and the ratio n/u between the number of variables and the number of input polynomials. For example, our algorithm permits to decompose polynomials of degree four in $\mathcal{O}(n^{12})$ if $n/u < 1/2$.

[1] `http://www.maplesoft.com/`

1.2. Organization of the Paper and Main Results

The paper is organized as follows. We begin in Section 2 by fixing some notations and introducing more formally the *Functional Decomposition Problem* (FDP) which is the main concern of this paper. In Section 3, we present an algorithm for decomposing polynomials of the same degree (i.e. all the polynomials of the mapping are of the same degree). Briefly, our algorithm works as follows. Let $h = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ be the polynomials obtained from the composition of $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big) \in \mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^n$, i.e.

$$(h_1, \ldots, h_u) = \big(f_1\big(g_1, \ldots, g_n\big), \ldots, f_u\big(g_1, \ldots, g_n\big)\big).$$

All known techniques for decomposing split the problem into two parts. First, compute candidates for the $g_1, \ldots, g_n$ and recover $f_1, \ldots, f_u$ from this knowledge. Note that determining $f_1, \ldots, f_u$ knowing $h_1, \ldots, h_u$ and $g_1, \ldots, g_n$ is a subfield membership problem (18; 27). This is a difficult problem in general. However, in our context, the degree of the polynomials are bounded. Therefore, linear algebra techniques can be used to recover the unknown coefficients of the f_is.

The harder step being usually to recover candidates for $g_1, \ldots, g_n$. The aim of our algorithm is to find the vector space $\mathcal{L}(g) = \mathrm{Span}_{\mathbb{K}}(g_1, \ldots, g_n)$ generated by $g_1, \ldots, g_n$. This vector space will be computed from the reduced DRL Gröbner bases of suitable ideals. More precisely, we will consider a sequence of quotient ideals constructed from the ideal generated by the partial derivatives of h_i, i.e. :

$$\partial\mathcal{I}_h = \left\langle \frac{\partial h_i}{\partial x_j} \right\rangle_{1 \le i \le u}^{1 \le j \le n}.$$

As soon as the decomposition is unique – in a sense that we will precise in Definition 2 – our technique allows to recover in most cases (see Remark 4) a basis of $\mathcal{L}(g)$.

In Section 4, we will describe the application that initially motivated this work, namely $2R^-$ schemes (16; 17). The security of these schemes is based on the (expected) practical difficulty of FDP. We present some experimental results obtained with our algorithm on real size instances of FDP corresponding to $2R^-$ schemes. We will see that the efficiency of our approach render the principle of two-round schemes, and probably any extension, obsolete.

2. The Functional Decomposition Problem

In this part, we introduce more formally the problem of decomposing multivariate polynomials. Let $h = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ be a set of multivariate polynomials. We shall say that $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big) \in \mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^n$ is a *decomposition* of h if:

$$h = \big(h_1, \ldots, h_u\big) = \big(f_1\big(g_1, \ldots, g_n\big), \ldots, f_u\big(g_1, \ldots, g_n\big)\big) = f \circ g.$$

Observe that taking $h = f$ and $g = (g_1, \ldots, g_n) = (x_1, \ldots, x_n)$, or $f = (x_1, \ldots, x_u)$ and $g = (h_1, \ldots, h_u, 0, \ldots, 0)$ will lead to a valid, but trivial, decomposition of h. Another "pathological" case can be obtained as follows. Let $g = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$

be an automorphism (9) polynomial map, i.e. a map for which there exists another polynomial map $\tilde{g} = (\tilde{g}_1, \ldots, \tilde{g}_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$ such that :

$$x_i = \tilde{g}_i(g_1, \ldots, g_n), \text{for all } i \leq 1 \leq i \leq n.$$

It follows that any polynomial map $h = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ has a decomposition $h = f \circ g$, where f is given by :

$$f_i = h_i(\tilde{g}_1, \ldots, \tilde{g}_n), \text{for all } i \leq 1 \leq i \leq u.$$

From this short discussion, we can remark that it is not so obvious to define a notion of non trivial decomposition. In (19), the authors considered that a non trivial decomposition is a decomposition $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big) \in \mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^n$ of $h = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ if :

$$\mathbb{K}[h_1, \ldots, h_u] \subset \mathbb{K}[g_1, \ldots, g_n] \subset \mathbb{K}[x_1, \ldots, x_n].$$

Even with these restrictions, you can get "trivial" decompositions. In particular, if the transcendence degree of the rational field $\mathbb{K}(x_1, \ldots, x_n)$ over the unirational field $\mathbb{K}(h_1, \ldots, h_n)$ is smaller than n (19; 20). To handle this problem, we will use the notion of genericity.

Definition 1. Let $E_{\mathbb{K}}(u, n, d)$ be the set of all polynomials $p_1, \ldots, p_u \in \mathbb{K}[x_1, \ldots, x_n]$ being of degree smaller (or equal) to d respectively. We shall say that a property is **generic** if it holds over a non empty Zarisky's open, i.e. if the property is verified for all sequences in $E_{\mathbb{K}}(u, n, d)$ except for an algebraic set of co-dimension at least one. We shall also say that a polynomial is **generic** if their coefficients are considered as algebraic polynomials.

In order to avoid trivial cases, we shall say in this paper that a decomposition $(f, g) \in \mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^n$ of $h \in \mathbb{K}[x_1, \ldots, x_n]^u$ is *generically non trivial* is f, g and h have degrees greater than one and the coefficients of (f, g) are generics. Here, the degree of a polynomial map $p = (p_1, \ldots, p_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ is the maximal degree of the monomials occurring in the p_is. The *Functional Decomposition Problem* (FDP) is then as follows :

FDP

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

Find : – if any – a generic non trivial decomposition $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big)$ $\in \mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^n$ of h.

From now on, we will simply call a generic non trivial decomposition a trivial decomposition; i.e. the notion of genrericity will be always assumed in this case.

A decomposition $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big)$ of $h = (h_1, \ldots, h_u)$ can not be unique. Indeed, any bijective linear combination A of the g_is leads to a decomposition of h since:

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

This suggests to introduce the following notion of uniqueness (18).

Definition 2. Let $h = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$. We shall say that :

- two decompositions $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big)$ and $\big(\tilde{f} = (\tilde{f}_1, \ldots, \tilde{f}_u), \tilde{g} = (\tilde{g}_1, \ldots, \tilde{g}_n)\big)$ of h are *equivalent* if $\exists A \in GL_n(\mathbb{K})$ such that $\tilde{g} = g \cdot A$.
- a decomposition (f, g) of h is *unique* if all decompositions are equivalent.

In order to simplify our task, we will consider a slightly modified version of FDP. First, we will suppose that the input polynomials are homogeneous of the same degree. Moreover, we will suppose that the degrees of a decomposition is part of the input.

To summarize, let d_h, d_f, d_g be positive integers strictly greater than one.

FDP(d_h, d_f, d_g)

Input : $h = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$, with the h_is all of degree d_h.

Find : – if any – homogeneous polynomials $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big) \in$ $\mathbb{K}[x_1, \ldots, x_n]^u \times \mathbb{K}[x_1, \ldots, x_n]^n$ of degree d_f and d_g respectively such that $h = f \circ g$.

We shall say that (f, g) is a (d_f, d_g)-*decomposition* of h if (f, g) is a decomposition of h, and $\deg(f) = d_f$, $\deg(g) = d_g$. Finally, we now recall the definition of an ideal quotient (or colon ideal), which is an important ingredient of our algorithm (9).

Definition 3. Let $\mathcal{I}$ and $\mathcal{J}$ be ideals of $\mathbb{K}[x_1, \ldots, x_n]$. The **ideal quotient** of $\mathcal{I}$ by $\mathcal{J}$, denoted $\mathcal{I} : \mathcal{J}$, is the set

$$\mathcal{I} : \mathcal{J} = \big\{f \in \mathbb{K}[x_1, \ldots, x_n] : f \cdot g \in \mathcal{I}, \text{ for all } g \in \mathcal{J}\big\}.$$

If $\mathcal{J} =< f >$, we will simply denote $\mathcal{I} : f$. A (Gröbner) basis (6; 7) of a quotient ideal can be computed using standard elimination techniques (1; 9). In our context, we will see that such Gröbner basis can be computed using a more simple method.

3. An Algorithm for Solving FDP

In this part, we will present an algorithm for solving FDP(d_h, d_f, d_g), with $d_h, d_f, d_g > 1$.

3.1. The Homogeneous Case

We first remark that we can w.l.o.g. restrict our attention to homogeneous instances of FDP. We shall call *homogenization* of $p \in \mathbb{K}[x_1, \ldots, x_n]$ the polynomial $p^*(x_0, x_1, \ldots, x_n) = x_0^{deg(p)} p(x_1/x_0, \ldots, x_n/x_0)$, where x_0 is a new variable.

Lemma 1. *(31) Let $f = (f_1, \ldots, f_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ and $g = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$, with all the polynomials of f (resp. g) of degree d_f (resp. d_g). We have :*

$$(f \circ g)^* = f^* \circ g^*,$$

with $f^* = (x_0^{d_f}, f_1^*, \ldots, f_u^*)$ and $g^* = (x_0^{d_g}, g_1^*, \ldots, g_n^*)$.

Proof. We have :

$$f^*(x_0, x_1, \ldots, x_n) = \big(x_0^{d_f}, x_0^{d_f} f_1(x_1/x_0, \ldots, x_n/x_0), \ldots, x_0^{d_f} f_u(x_1/x_0, \ldots, x_n/x_0)\big),$$
$$g^*(x_0, x_1, \ldots, x_n) = \big(x_0^{d_g}, x_0^{d_g} g_1(x_1/x_0, \ldots, x_n/x_0), \ldots, x_0^{d_g} g_n(x_1/x_0, \ldots, x_n/x_0)\big).$$

Therefore :

$$f^* \circ g^* = \left(x_0^{d_f \cdot d_g}, x_0^{d_f \cdot d_g} f_1(g_1^*/x_0^{d_g}, \ldots, g_n^*/x_0^{d_g}), \ldots, x_0^{d_f \cdot d_g} f_1(g_1^*/x_0^{d_g}, \ldots, g_n^*/x_0^{d_g}),\right.$$

which is exactly equal to $(f \circ g)^*$. $\square$

Thus, if (f^*, g^*) is a decomposition of h^*, then a decomposition (f, g) of h is obtained by dehomogenization of f^* and g^*, i.e. by computing $f^*(1, x_1, \ldots, x_n)$ and $g^*(1, x_1, \ldots, x_n)$.

From now on, we assume that $f = (f_1, \ldots, f_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$ and $g = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$ are homogeneous polynomials of degree d_f and d_g respectively. Note that $h = (h_1, \ldots, h_u) = f \circ g$ will be given by homogeneous polynomials of degree $d_h = d_f \cdot d_g$.

3.2. Description of the Algorithm

The algorithm is divided in two parts. First, we try to recover the vector space $\mathcal{L}(g) = \mathrm{Span}_{\mathbb{K}}(g_1, \ldots, g_n)$ generated by $g = (g_1, \ldots, g_n)$. This linear span will be recovered from the DRL Gröbner bases of suitable ideals. Secondly, we deduce a decomposition (f, g) of h from $\mathcal{L}(g)$.

3.2.1. The second step – a simple linear algebra step

To do so, we remark that the knowledge of $\mathcal{L}(g)$ is sufficient for decomposing h. Indeed, suppose that $g = (g_1, \ldots, g_n)$ is a basis of $\mathcal{L}(g)$. The symbolic equalities :

$$h_i = f_i(g_1, \ldots, g_n), \text{for all } i, 1 \leq i \leq u, \tag{1}$$

permit, by comparing the coefficients in the right-most and left-most parts of these equalities, to obtain a linear system of $\mathcal{O}(u \cdot \mathrm{C}_{n+d_f}^{d_f})$ equations in the $u \cdot \mathrm{C}_{n+d_f}^{d_f}$ unknown coefficients of the f_is. Any solution of this linear system will provide a valid decomposition. On the other hand, if this system has no solution, we can conclude that there exists no valid decomposition exists. It remains to determine the vector space $\mathcal{L}(g)$.

3.2.2. The first step – recovering the linear span

First, we will briefly recall the approach of (14) for finding a $(2, 2)$ decomposition. In this context, we can write :

$$f_i = \textstyle\sum_{1 \leq k, \ell \leq n} f_{k,\ell}^{(i)} x_k x_\ell \in \mathbb{K}[x_1, \ldots, x_n], \text{ for all } i, 1 \leq i \leq u,$$
$$g_i = \textstyle\sum_{1 \leq k, \ell \leq n} g_{k,\ell}^{(i)} x_k x_\ell \in \mathbb{K}[x_1, \ldots, x_n], \text{ for all } i, 1 \leq i \leq n.$$

Therefore, for all $i, 1 \leq i \leq u$:

$$h_i = f_i(g_1, \ldots, g_n) = \sum_{1 \leq k, \ell \leq n} f_{k,\ell}^{(i)} g_k g_\ell. \tag{2}$$

We then observe that :

$$\frac{\partial h_i}{\partial x_j} = \sum_{1 \leq k, \ell \leq n} f_{k,\ell} \left(\frac{\partial g_k}{\partial x_j} g_\ell + \frac{\partial g_\ell}{\partial x_j} g_k \right). \tag{3}$$

The polynomials $g_1, \ldots, g_n$ being of degree two, their partial derivatives $\frac{\partial g_k}{\partial x_j}$ are of degree one. Hence :

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

As we will see, this ideal usually provides enough information for recovering a basis of $\mathcal{L}(g)$.

Theorem 1. Let $\mathrm{M}(d)$ be the set of monomials of degree $d \geq 0$ in $x_1, \ldots, x_n$, and :

$$C_d = \{m \times g_k : m \in \mathrm{M}(d+1), \text{ and } k, 1 \leq k \leq n\},$$
$$R_d = \left\{ m \times \frac{\partial h_i}{\partial x_j} : m \in \mathrm{M}(d), 1 \leq i \leq u, \text{ and } j, 1 \leq j \leq n \right\}.$$

If $\dim(\mathrm{Span}_{\mathbb{K}}(R_d)) \geq \#C_d$, there exists $d \geq 0$ such that for all $i, 1 \leq i \leq n$:

$$x_n^{d+1} g_i \in \partial \mathcal{I}_h,$$

Proof. According to (3), we have for all $m \in \mathrm{M}(d)$:

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

Again, we recall that the partial derivatives $\frac{\partial g_k}{\partial x_j}$ are of degree one. We then deduce that each polynomial of R_d can be written as a sum of elements in :

$$C_d = \{m \times g_k : m \in \mathrm{M}(d+1), \text{ and } k, 1 \leq k \leq n\},$$

It is then natural to consider the matrix whose rows are indexed by the polynomials $m \times \frac{\partial h_i}{\partial x_j} \in R_d$, and columns by the elements of C_d. Namely :

$$A = \begin{array}{c} \\ \vdots \\ \vdots \\ m \times \frac{\partial h_i}{\partial x_j} \\ \vdots \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccc} \cdots & \cdots & m \times g_k & \cdots & \cdots \end{array} \\ \begin{pmatrix} & \cdots & & & \\ & \cdots & & & \\ & \cdots & & & \\ & \cdots & & & \\ & \cdots & & & \end{pmatrix} \end{array}$$

Thus, $x_n^{d+1} g_i \in \mathrm{Span}_{\mathbb{K}}(R_d) \subset \partial \mathcal{I}_h$, for all $i, 1 \leq i \leq n$. Indeed, $\dim(\mathrm{Span}_{\mathbb{K}}(R_d))$ – the number of linearly independent rows of A – is at least equal to $\#C_d$; the number of columns of A. □

We will now see how we can extend this idea for decomposing polynomials of arbitrary degree. To do so, we consider the problem of recovering $\mathcal{I} = \langle q_1, \ldots, q_u \rangle$ from the knowledge of $\mathcal{I}^k$, i.e. computing the k-th root of $\mathcal{I}^k$. This problem can be viewed as a special decomposition problem. Obviously, we can assume that $\mathcal{I}^k$ is generated by all the products of the form $q_{i_1} q_{i_2} \cdots q_{i_k}, 1 \leq i_1, i_2, \ldots, i_k \leq u$. In order to ease the exposure, we introduce the following :

Definition 4. Let k be a positive integer. We will denote by $p_{i,k}$ a product of k (not necessarily distinct) polynomials q_js, i.e. a product of the form :

$$q_{j_1} q_{j_2} \cdots q_{j_k}, 1 \leq j_1, j_2, \ldots, j_k \leq u.$$

We will also denote by r_k the number of such products.

We would like to emphasize that we will extensively use these notations in the following.

Remark 2. For $k = 2$, we have for instance :

$$\mathcal{J}_2 = \langle q_j q_k \rangle_{1 \leq j \leq k \leq u},$$

and $r_2 = n(n+1)/2$.

Obverse that each $p_{i,k}$ can be obtained from the composition of a monomial of degree k by $q_1, \ldots, q_n$. We will now extend the formula (3) in a more general context. To this end, we remark that :

$$\frac{\partial p_{i,k}}{\partial x_r} = \frac{\partial}{\partial x_r}(q_{j_1} q_{j_2} \cdots q_{j_k}) = \sum_{s=1}^{k} \frac{\partial q_{j_s}}{\partial x_r} \prod_{t=1,\, t \neq s}^{k} q_{j_t}. \tag{4}$$

This will permit to prove the following result :

Lemma 3. *Let $k > 1, \mathrm{M}(d)$ be the set of monomials of degree $d \geq 0$ in $x_1, \ldots, x_n$, and $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal generated by homogeneous polynomials of the same degree $d_{\mathcal{I}} > 1$. Let also $\mathcal{I}^k =< p_{i,k} >_{1 \leq i \leq r_k}$ and $\mathcal{I}^{k-1} =< p_{i,k-1} >_{1 \leq i \leq r_{k-1}}$ be the k-th power and $(k-1)$-th power of $\mathcal{I}$ respectively (notations as in Definition 4). Finally, we set :*

$$C_{k-1} = \left\{ m' \times p_{i,k-1} : m' \in \mathrm{M}(d_{k-1} + d_{\mathcal{I}} - 1) \text{ and } i, 1 \leq i \leq r_{k-1} \right\},$$
$$R_{k-1} = \left\{ m \times \frac{\partial p_{i,k}}{\partial x_j} : m \in \mathrm{M}(d_{k-1}), 1 \leq i \leq r_k, \text{ and } j, 1 \leq j \leq n \right\}.$$

If $\dim\big(\mathrm{Span}_{\mathbb{K}}(R_{k-1})\big) \geq \#C_{k-1}$, for some $d_{k-1} \geq 1$, then :

$$x_n^{d_{\mathcal{I}}-1+d_{k-1}} \cdot p_{i,k-1} \in \partial\mathcal{I}^k, \text{ for all } i, 1 \leq i \leq r_{k-1}.$$

$\partial\mathcal{I}^k$ being the ideal generated by the first order partial derivatives of $\mathcal{I}^k$s generators, i.e.

$$\partial\mathcal{I}^k = \left\langle \frac{\partial p_{i,k}}{\partial x_j} \right\rangle_{1 \leq i \leq r_k}^{1 \leq j \leq n}$$

Proof. According to (4), we can suppose that each generator of $\partial\mathcal{I}^k$ can be written as :

$$\sum_{i=1}^{r_{k-1}} a_{i,k-1} m_{i,k-1} p_{i,k-1},$$

with $a_{i,k-1} \in \{0, 1\}$ and $m_{i,k-1}$ being a monomial of degree $d_{\mathcal{I}} - 1$. This means that the partial derivatives $\frac{\partial p_{i,k}}{\partial x_j}$ are in $\mathcal{I}^{k-1}$.

Let then $m \in \mathrm{M}(d_{k-1})$. Obviously, each polynomial $m \times \frac{\partial p_{i,k}}{\partial x_j}$ can be expressed as the sum of monomials $m'_{i,k-1}$ of degree $d_{k-1} + d_{\mathcal{I}} - 1$ by some $p_{i,k-1}$. We then consider the matrix, denoted A_{k-1}, whose :

- rows are labeled by the polynomials of :

$$R_{k-1} = \left\{ m \times \frac{\partial p_{i,k}}{\partial x_j} : m \in \mathrm{M}(d_{k-1}), 1 \leq i \leq r_k, \text{ and } j, 1 \leq j \leq n \right\}.$$

- columns are labeled by the polynomials of :

$$C_{k-1} = \left\{ m' \times p_{i,k-1} : m' \in \mathrm{M}(d_{k-1} + d_{\mathcal{I}} - 1) \text{ and } i, 1 \leq i \leq r_{k-1} \right\}.$$

In this setting, the coefficient in A_{k-1} corresponding to the row $m \times \frac{\partial p_{i,k}}{\partial x_j}$ and column $m' \times p_{i,k-1}$ is the coefficient of $m' \times p_{i,k-1}$ in the polynomial $m \times \frac{\partial p_{i,k}}{\partial x_j}$. In other words :

$$A_{k-1} = \begin{array}{c} \\ \vdots \\ \vdots \\ m \times \frac{\partial p_{i,k}}{\partial x_j} \\ \vdots \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccc} \cdots & \cdots & m' \times p_{i,k-1} & \cdots & \cdots \end{array} \\ \begin{pmatrix} & \cdots & \\ & \cdots & \\ & \cdots & \\ & \cdots & \\ & \cdots & \end{pmatrix} \end{array}$$

Since $\dim\big(\mathrm{Span}_{\mathbb{K}}(R_{k-1})\big)$ is at least equal to $\#C_{k-1}$, it holds that :

$$x_n^{d_{\mathcal{I}}-1+d_{k-1}} \cdot p_{i,k-1} \in \partial\mathcal{I}^k \text{ for all } i, 1 \leq i \leq r_{k-1},$$

concluding the proof. □

We would like to emphasize that Lemma 3 allows to compute the k-th root of $\mathcal{I}^k$. We will see that $\mathcal{I}$ can be recovered by computing the successive quotient ideals :

$$\partial\mathcal{I}^k : x_n^{d_{k-1}+d_{\mathcal{I}}-1}, \partial\mathcal{I}^{k-1} : x_n^{d_{k-2}+d_{\mathcal{I}}-1}, \ldots, \partial\mathcal{I}^2 : x_n^{d_1+d_{\mathcal{I}}-1},$$

for some integers $d_{k-1}, d_{k-2}, \ldots, d_1 \geq 1$. Typically, we can recover $\mathcal{I}^{k-1}$ by computing $\partial\mathcal{I}^k : x_n^{d_{k-1}+d_{\mathcal{I}}-1}$ using standard Gröbner bases techniques, and then from Lemma 3 :

$$\mathcal{I}^{k-1} \subseteq \partial\mathcal{I}^k : x_n^{d_{k-1}+d_{\mathcal{I}}-1},$$

Remark also that $\mathbb{K}[x_1, \ldots, x_n]$ being noetherian, we know that there exists $d^* < \infty$ such that, for all $j, 1 \leq j \leq k$:

$$\cdots \subseteq \partial\mathcal{I}^j : x_n^{d^*-1} \subseteq \partial\mathcal{I}^j : x_n^{d^*} = \partial\mathcal{I}^j : x_n^{d^*+1}.$$

Thus, $d_{k-1}, d_{k-2}, \ldots, d_1$ are obviously bounded from above by d^*. We will provide a generic lower bound on these parameters at the end of this part. Now, we extend Lemma 3 to obtain the main result of this section.

Theorem 2. Let $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big)$ be a (d_f, d_g)-decomposition of $h = (h_1, \ldots, h_u)$ and $\mathcal{I}_h = \langle h_1, \ldots, h_u \rangle =< p_{i,d_f} >_{1 \leq i \leq r_{d_f}}$, with $r_{d_f} = u$. Let also $\mathcal{I}_g = \langle g_1, \ldots, g_n \rangle$. For all $k, 1 < k < d_f$, we will denote by $p_{i,k}$ a product of k (not necessarily distinct) polynomials g_js, i.e. a product of the form :

$$g_{j_1} g_{j_2} \cdots g_{j_k}, 1 \leq j_1, j_2, \ldots, j_k \leq n.$$

We will also denote by r_k the number of such products. Thus, we have $\mathcal{I}_g^k =< p_{i,k} >_{1 \leq i \leq r_k}$. Finally, we set for all $k, 1 < k \leq d_f$:

$$C_{k-1} = \big\{m' \times p_{i,k-1} : m' \in \mathrm{M}(d_{k-1} + d_g - 1), \text{and } i, 1 \leq i \leq r_{k-1}\big\},$$
$$R_{k-1} = \left\{m \times \frac{\partial p_{i,k}}{\partial x_j} : m \in \mathrm{M}(d_{k-1}), 1 \leq i \leq r_k, \text{and } j, 1 \leq j \leq n\right\}.$$

Therefore, for all $k, 1 < k \leq d_f$:

$$x_n^{d_g-1+d_{k-1}} \cdot p_{i,k-1} \in \partial\mathcal{I}_g^k, \text{ for all } i, 1 \leq i \leq r_{k-1}, \tag{5}$$

if there exists $d_{k-1} \geq 1$, such that $\dim\big(\mathrm{Span}_{\mathbb{K}}(R_{k-1})\big) \geq \#C_{k-1}$.

Proof. The proof is essentially the same as the one presented in Lemma 3. The more important fact is to remark that $\mathcal{I}_h \subseteq \mathcal{I}_g^{d_f}$. We have then simply replaced $\mathcal{I}^{d_f}$ by $\mathcal{I}_h$. □

The set $\mathcal{L}(g) \subset \mathcal{I}_g$ can be extracted from the quotient ideals :

$$\mathcal{Q}_{d_f-1} = \partial\mathcal{I}_h : x_n^{d_{d_f-1}+d_g-1}, \ldots, \mathcal{Q}_3 = \partial\mathcal{I}_g^3 : x_n^{d_2+d_g-1}, \mathcal{Q}_2 = \partial\mathcal{I}_g^2 : x_n^{d_1+d_g-1},$$

for suitably chosen positive integers $d_{d_f-1}, \ldots, d_2, d_1$. The ideal $\mathcal{I}_h$ being homogeneous, all these quotients are also homogeneous ideals. Moreover :

$$\min\big(deg(p) : p \in \mathcal{Q}_{k-1}\big) = (k-1)d_g, \text{for all } k, 1 < k \leq d_f.$$

Let G_{k-1} be a (reduced) DRL Gröbner basis of $\mathcal{Q}_{k-1}$ and let $B_{k-1}(g)$ be the set of polynomials of G_{k-1} of degree $(k-1)d_g$, i.e. :

$$B_{k-1}(g) = \big(g \in G_{k-1} : deg(g) = (k-1)d_g\big).$$

According to the minimality – w.r.t. the degree – of a DRL Gröbner basis :

$$\mathrm{Span}_{\mathbb{K}}\big(B_{k-1}(g)\big) = \mathrm{Span}_{\mathbb{K}}\big(g \in \mathcal{Q}_{k-1} : deg(g) = (k-1)d_g\big), \text{for all } k, 1 < k \leq d_f.$$

In particular, we get from Theorem 2 that $\mathcal{L}(g) \subseteq \mathrm{Span}_{\mathbb{K}}\big(B_1(g)\big)$. When the decomposition is unique, $\mathcal{L}(g)$ is of dimension n generically. Consider the matrix A_g whose row $i, 1 \leq i \leq n$ is filled by the coefficients of g_i (w.r.t some ordering). The fact that $\dim\big(\mathcal{L}(g)\big) < n$ implies that the matrix A_g is not of full rank, which can be expressed by the vanishing of an algebraic system via the minors of A_g. To show that this set is non empty, we can take for instance $g = (g_1, \ldots, g_n)$. Remark that $\dim\big(\mathrm{Span}_{\mathbb{K}}\big(B_1(g)\big)\big) = n$ implies that $\mathcal{L}(g) = \mathrm{Span}_{\mathbb{K}}\big(B_1(g)\big)$.

3.2.3. Computing the quotient ideal

In this part, we will explain a simple way to compute a basis of $\partial\mathcal{I}_g^k : x_n^{d_{k-1}+d_g-1}$. Precisely, we will describe an explicit way for computing the set $B_{k-1}(g)$, for all $k, 1 < k \leq d_f$. To do so, we recall that the variable x_n has a particular property in a DRL order. Indeed, it is well known that if $x_n^{d_{k-1}+d_g-1}$ divides the leading monomial of a polynomial, then it will also divide the whole polynomial. Thus, we can restrict our attention to the polynomials of a $(k \cdot d_g + d_{k-1} - 1)$-DRL Gröbner bases G'_{k-1} of $\partial\mathcal{I}_g^k$ (or $\partial\mathcal{I}_h$, if $k = d_f$) whose leading monomial are divided by $x_n^{d_{k-1}+d_g-1}$. Precisely :

$$B_{k-1}(g) = \left(\frac{g'}{x_n^{d_{k-1}+d_g-1}} : g' \in G'_{k-1}, \text{and } x_n^{d_{k-1}+d_g-1} \mid \mathrm{LM}(g', \prec_{DRL})\right).$$

$\mathrm{LM}(g', \prec_{DRL})$ being the leading monomial of g' w.r.t. the DRL order.

3.3. The Algorithm MultivariateComPoly

We are now in a position to describe our algorithm.

MultivariateComPoly

Input: d_f, d_g, d_h and u homogeneous polynomials $h = (h_1, \ldots, h_u)$ of the same degree d_h

Output : `Fail`, or a non trivial decomposition $\big(f = (f_1, \ldots, f_u), g = (g_1, \ldots, g_n)\big)$ of h

$G = \{g_1, \ldots, g_k\} \leftarrow$ **InsideComp**$\big(d_f, d_g, d_h, h = (h_1, \ldots, h_u)\big)$

`// The polynomials of` G `form a vector basis of` $\mathcal{L}(g)$

If $k \neq n$ **then** Return `Fail`

Compute the set Sys of solutions of the linear system generated, as explained in (1), from g

If $\#Sys = 0$ **then** Return `No Decomp` `// no non trivial decomposition`

Else Pick a random element $f = (f_1, \ldots, f_u)$ of Sys

`//` $h = f \circ g$`, for any` $f = (f_1, \ldots, f_u)$ `corresponding to an element of` Sys

Return $\big(g = (g_1, \ldots, g_n), f = (f_1, \ldots, f_u)\big)$

Remark 4. This algorithm returns `Fail` when $\mathcal{L}(g) \neq \mathrm{Span}_{\mathbb{K}}(G)$. This can be due to the fact that the decomposition is not unique, or simply because $\mathrm{Span}_{\mathbb{K}}(G)$ can contain polynomials $g \notin \mathcal{L}(g)$. Anyway, all the generators of $\mathcal{L}(g)$ are contained in G . Thus, one can performs an exhaustive search over the polynomials of G to recover a basis of $\mathcal{L}(g)$. In theory, our approach can be extended for decomposing polynomials having several decompositions. But, most of the instances of FDP that we solved in our experiments have an unique decomposition. For this reason, we have chosen to present this version of the algorithm, which is very close to our actual implementation.

The procedure **InsideComp**, which is the core of the algorithm, recover – if any – a basis of the linear span $\mathcal{L}(g)$.

InsideComp

Input: d_f, d_g, d_h and u homogeneous polynomials $h_1, \ldots, h_u$ of same degree d_h

Output : `Fail`, or a linear basis of $\mathcal{L}(g)$

$\mathcal{I}_{d_f}(h) \leftarrow \langle h_1, \ldots, h_u \rangle$

For k from d_f to 2 **do**

Find the smallest integer d_{k-1} such that $\dim\big(\mathrm{Span}_{\mathbb{K}}(R_{k-1})\big) \geq \#C_{k-1}$ `// notations as in Theorem 2`

Compute a reduced $(k \cdot d_g + d_{k-1} - 1)$-DRL Gröbner bases G'_{k-1} of $\partial\mathcal{I}_k(h)$

$B_{k-1} \leftarrow \left(\frac{g'}{x_n^{d_{k-1}+d_g-1}} : g' \in G'_{k-1}, \text{and } x_n^{d_{k-1}+d_g-1} \mid \mathrm{LM}(g', \prec_{DRL}) \right)$

$\partial\mathcal{I}_{k-1}(h) \leftarrow \left\langle \frac{\partial g}{\partial x_j} : g \in B_{k-1}, 1 \leq j \leq n \right\rangle$

od

Return B_1

Remark 5. Let $k > 1$, and $\mathcal{I}^k =< p_{i,k} >_{1\leq i\leq r_k}$ be the k-th power of an ideal $\mathcal{I} = \langle g_1, \ldots, g_n\rangle$. Remark that $\mathbf{InsideComp}\big(k, d_g, k{\cdot}d_g, \{p_{i,k}\}_{1\leq i\leq r_k}\big)$ returns a DRL Gröbner basis of $\mathcal{I}$.

3.3.1. Complexity

In this part, we investigate the complexity of **MultivariateComPoly**.

Theorem 3. Let the notations be as in Theorem 2. For all $k, 1 < k \leq d_f$, let d_{k-1} be the smallest integer such that $\dim\big(\mathrm{Span}_{\mathbb{K}}(R_{k-1})\big) \geq \#C_{k-1}$. The complexity of **MultivComPoly** is :

$$\mathcal{O}\left(\sum_{k=2}^{d_f} n^{3\left(k\cdot d_g + d_{k-1}-1\right)}\right).$$

Proof. The complexity of $\mathrm{Algo}_{\mathrm{FDP}}$ is dominated by the cost of **InsideComp**. That is, the cost of computing the reduced DRL Gröbner basis G_{k-1}, for all $k, 1 < k \leq d_f$. As explained in 3.2, this can be done by computing a $(k\cdot d_g + d_{k-1} - 1)$-DRL Gröbner bases of $\partial\mathcal{I}_k^h$. We recall that we have homogeneous polynomials. Thus, according to (22; 23), such basis can be computed using F_5 (12) in $\mathcal{O}(n^{3(k\cdot d_g + d_k - 1)})$, for each $k, 1 < k \leq d_f$. □

It is important to know the exact value of the parameters $d_{d_f-1}, \ldots, d_2, d_1$. We will provide a lower-bound on these values. Generically, we can say that the vectors of :

$$R_{k-1} = \left\{ m \times \frac{\partial p_{i,k}}{\partial x_j} : m \in \mathrm{M}(d_{k-1}), 1 \leq i \leq r_k, \text{and } j, 1 \leq j \leq n \right\}, \text{for all } k, 1 < k \leq d_f.$$

are linearly independent. Indeed, let $A_{R_{k-1}}$ be the matrix constructed from the elements of R_{k-1} $\big($viewed over the vector space generated by the monomials of degree $d_{k-1}\cdot k\cdot d_g\big)$. Then, the fact that the vectors of R_{k-1} are not linearly independent implies that the matrix $A_{R_{k-1}}$ is not of full rank, which can be expressed by the vanishing of an algebraic system via the minors of $A_{R_{k-1}}$ (by viewing the polynomials $p_{i,k}$s as generic polynomials).

Thus, $\dim\big(\mathrm{Span}_{\mathbb{K}}(R_{k-1})\big) = n \cdot r_k \cdot \mathrm{C}_{n+d_{k-1}}^{d_{k-1}}$. Therefore, we get that the parameters $d_{d_f-1}, \ldots, d_2, d_1$ must be chosen such that :

$$n \cdot r_k \cdot \mathrm{C}_{n+d_{k-1}}^{d_{k-1}} \geq \#C_{k-1} = r_{k-1} \cdot \mathrm{C}_{n+d_{k-1}+d_g-1}^{d_{k-1}+d_g-1}.$$

Therefore, for all $k, 1 < k \leq d_f, d_{k-1}$ will be generically equal to the smallest integer such that :

$$\mathrm{C}_{n+d_{k-1}}^{d_{k-1}} \geq \frac{r_{k-1}}{n \cdot r_k} \cdot \mathrm{C}_{n+d_{k-1}+d_g-1}^{d_{k-1}+d_g-1}.$$

Remark that $r_{d_f} = u$, and $r_1 = n$. For all $k, 1 < k < d_f$, we can also take :

$$r_k = \mathrm{C}_n^k.$$

In the cryptographic application that initially motivated this work, we have $d_f = d_g = 2$. In this case, we have obtained (14) that :

Property 1. Let the notations be as in Theorem 2. We set $d_f = d_g = 2$. Thus, d_1 must verify :

$$d_1 \geq \frac{n}{u} - 1.$$

We then obtain :

Corollary 1. Let the notations be as in Theorem 2. We set $d_f = d_g = 2$. If the number $u \geq \lfloor \frac{n}{2} \rfloor$, the complexity of **MultivariateComPoly** is $\mathcal{O}(n^{12})$, and $\mathcal{O}(n^9)$ if $u = n$.

We will show now that this is perfectly coherent with our experimental results.

4. Application to Cryptography

We present in this part some experimental results obtained with our algorithm. We will mainly focus our attention to the application that initially motivated this work : the cryptanalysis of $2R^-$ schemes (16; 17).

4.1. One-Round and Two-Rounds Schemes

In (24), Matsumoto and Imai have proposed the first efficient public key cryptosystem based on multivariate polynomials. The public key $p = (p_1, \ldots, p_n) \in \mathbb{F}_2[x_1, \ldots, x_n]^n$ of this scheme – called C^* (25) – is a set of multivariate polynomials obtained from the composition of a carefully chosen quadratic multivariate system $\psi = (\psi_1, \ldots, \psi_n) \in \mathbb{F}_2[x_1, \ldots, x_n]^n$ by two secret linear (invertible) transformations $(S, T) \in GL_n(\mathbb{F}_2) \times GL_n(\mathbb{F}_2)$, namely :

$$p(x_1, \ldots, x_n) = \psi\big((x_1, \ldots, x_n)S\big)T.$$

The polynomials of ψ are equal to the n components of $\phi \circ f \in \mathbb{F}_2[x_1, \ldots, x_n]^n$, where [2] $f(X) = X^{1+2^\theta} \in \mathbb{F}_{2^n}[X]$, and ϕ is an isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$.
To encrypt a message $m \in \mathbb{F}_2^n$, we compute $p(m)$. To decrypt a ciphertext $c \in \mathbb{F}_2^n$, we use the knowledge of the secret key (S, T), as well as the particular shape of ψ, to find a $m \in \mathbb{F}_2^n$ for which $c = p(m)$. This is merely equivalent to finding a root of the univariate polynomial $f(X) = X^{1+2^\theta} \in \mathbb{F}_{2^n}[X]$.

After this pioneer work of Matsumoto and Imai (24), several others constructions have been proposed for finding a suitable ψ, leading to a family of cryptosystems called *one-round schemes* (16; 17). Unfortunately, serious weaknesses have been found on several one-round schemes (26; 16; 17).

To strengthen these schemes, without modifying too much the basic principle, Patarin and Goubin introduced a new family of cryptosystems : *two-round schemes* (16; 17). The public key such systems, which is given by polynomials of degree four, is obtained by composing the public polynomials of two different instances of one-round schemes. More formally, let $(S, T, U) \in GL_n(\mathbb{K}) \times GL_n(\mathbb{K}) \times GL_n(\mathbb{K})$ be a triple of (invertible) linear transformations, and two quadratic multivariate systems ψ and $\phi \in \mathbb{K}[x_1, \ldots, x_n]^n$. The public polynomials are :

$$p(x_1, \ldots, x_n) = \big(p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)\big) = \phi\Big(\psi\big((x_1, \ldots, x_n)S\big)T\Big)U.$$

When all the polynomials of p are given, this scheme is called 2R scheme. If only some of them are given, let's say $u < n$, it is called $2R^-$ scheme.

The fundamental issue behind this new construction is the following: *does composing two weak one-round schemes leads to a secure scheme ?* This is obviously related to the

[2] θ is chosen such that $\gcd(\theta, 2^n - 1) = 1$.

difficulty of computing a $(2,2)$-decomposition of the polynomials of the public key. Note that, an efficient method for finding this decomposition permits to split $2R^-$ (resp. 2R) schemes into two independent schemes given by quadratic polynomials. To break these schemes, we then only have to solve two quadratic systems. As mentioned by Patarin and Goubin (16; 17), this makes the principle of two-round schemes, including the minus modification, useless.

4.2. Experimental Results

Generation of the instances

We have only considered instances $h = f \circ g$ of FDP admitting a $(2,2)$-decomposition. We constructed these instances in the following way:

– $f = \psi\big((x_1, \ldots, x_n)S\big)T$, and $g = \phi\big((x_1, \ldots, x_n)\big)U$, with random linear transformations $(S, T, U) \in GL_n(\mathbb{K}) \times GL_n(\mathbb{K}) \times GL_n(\mathbb{K})$. Moreover, $\psi, \phi \subset \mathbb{K}[x_1, \ldots, x_n]^n$ are "S-box" systems (16; 17), i.e. of the form :

$$\big(S_1(x_1 \ldots, x_{n_1}), S_2(x_{n_1+1} \ldots, x_{n_1+n_2}), \ldots, S_b(x_{n_1+n_2+\cdots+n_{d-1}+1}, \ldots, x_n)\big),$$

where $n = \sum_i n_i$, and each $S_i \in \mathbb{K}[x_1, \ldots, x_n]^{n_i}$ is composed of quadratic polynomials. Note that we shall call b the number of blocks. We then remove $r \geq 0$ polynomials of h.

Programming language – Workstation

The experimental results have been obtained with a Xeon bi-processor 3.2 Hz, with 6 Gb of Ram. The instances of FDP have been generated using the Maple software [3]. We used an implementation of F_5 (12) for computing truncated Gröbner bases.

Table Notations

The following notations are used in the next table below:

– n, the number of variables

– b, the number of blocks

– n_i, the number of variables in each block

– q, the size of the field

– r, the number of polynomials removed

– $d_{theo} = \lceil \frac{n}{u} - 1 \rceil$, the predicted (see 3.3) value of d_1 for which **MultivariateComPoly** returns a solution

– d_{real}, the observed value of d for which **MultivariateComPoly** returns a solution

– T, the total running time of our algorithm

– q^n, the security bound of (17; 4) for $2R^-$ schemes.

Practical Results

[3] http://www.maplesoft.com/

n	b	n_i	r	q	d_{theo}	d_{real}	T	q^n
8	4	2	0	65521	0	0	0.0 s.	
8	4	2	4	65521	1	1	0.0 s.	$\approx 2^{64}$
8	4	2	5	65521	2	2	0.3 s.	$\approx 2^{64}$
8	4	2	6	65521	3	3	1.9 s.	$\approx 2^{64}$
10	5	2	5	65521	1	1	0.2 s.	$\approx 2^{80}$
10	5	2	6	65521	2	2	3.2 s.	$\approx 2^{80}$
10	5	2	7	65521	3	3	21.4 s.	$\approx 2^{80}$
10	5	2	8	65521	4	4	180.8 s.	$\approx 2^{80}$
12	3	4	0	65521	1	1	0.1 s.	
12	3	4	5	65521	1	1	0.9 s.	$\approx 2^{96}$
12	3	4	6	65521	1	1	0.9 s.	$\approx 2^{96}$
12	3	4	7	65521	2	2	20.5 s.	$\approx 2^{96}$
12	3	4	8	65521	2	2	25.2 s.	$\approx 2^{96}$
12	3	4	9	65521	3	3	414 s.	$\approx 2^{96}$
20	5	4	0	65521	0	0	1.6 s.	
20	5	4	5	65521	1	1	55.2 s.	$\approx 2^{160}$
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	0	65521	0	0	4.9 s.	
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	0	65521	0	0	31.3 s.	
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.	$\approx 2^{256}$

Interpretation of the results

We mention that $n = 16$ and $n = 32$ were two challenges proposed by the designers of $2R^-$ schemes (16; 17). First, we have observed that the parameters b and n_i of the S-box systems seem irrelevant for the complexity of our algorithm. We have also tested our approach for instances of FDP constructed with various forms of ψ, ϕ proposed in (16; 17) (C^*+S-Box functions, Triangular+S-Box functions,...) and several values of q. These results are very similar to the ones obtained for S-Box functions, and thus not quoted here. The main observation is that our

algorithm behaves exactly as predicted. That is, $d_{theo} = \lceil \frac{n}{u} - 1 \rceil$ is exactly equal to the d_{real} observed in practice.

5. Conclusion

In this paper, we have presented a general algorithm for decomposing mappings of arbitrary, but the same, degree (i.e. all the components of the mapping are of the same degree). It remains an open question to decompose mappings with components of different degrees. Another interesting question is to further investigate the subfield membership problem (18; 27) when the degree of the polynomials is not given.

References

[1] A.W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases.* Graduate Studies in Mathematics, Vol. 3, AMS, 1994.

[2] M. Bardet, J-C. Faugère, B. Salvy and B-Y. Yang. *Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems.* In MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry, 15 pages, 2005.

[3] M. Bardet, J-C. Faugère, and B. Salvy. *On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations.* In Proc. of International Conference on Polynomial System Solving (ICPSS), pp. 71–75, 2004.

[4] E. Biham. *Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes (2R).* Advances in Cryptology – CRYPTO 2000, Lecture Notes in Computer Science, vol. 1807, Springer–Verlag, pp. 408-416, 2000.

[5] J. Cade. *A New Public-Key Cipher which Allows Signatures.* Second S.I.A.M. Conference on Applied Linear Algebra, Raleigh. NC, 1985.

[6] B. Buchberger. *Gröbner Bases : an Algorithmic Method in Polynomial Ideal Theory.* Recent trends in multidimensional systems theory. Reider ed. Bose, 1985.

[7] B. Buchberger, G.-E. Collins, and R. Loos. *Computer Algebra Symbolic and Algebraic Computation.* Springer-Verlag, second edition, 1982.

[8] V. Carlier, H. Chabanne, and E. Dottax *Grey Box Implementation of Block Ciphers Preserving the Confidentiality of their Design.* Proceedings of BFCA'05, Rouen, 2005. Also available at `http://eprint.iacr.org/2004/188.ps`.

[9] D. A. Cox, J.B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer-Verlag. New York, 1992.

[10] M. Dickerson. *The functional Decomposition of Polynomials.* Ph.D Thesis, TR 89-1023, Departement of Computer Science, Cornell University, Ithaca, NY, July 1989.

[11] M. Dickerson. *General Polynomial Decomposition and the s-1-decomposition are NP-hard.* International Journal of Foundations of Computer Science, 4:2 (1993), pp. 147–156.

[12] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Casis without Reduction to Zero:* F_5. Proceedings of ISSAC, pp. 75–83. ACM press, July 2002.

[13] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. *Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering.* Journal of Symbolic Computation, 16(4), pp. 329–344, 1993.

[14] J.-C. Faugère, L. Perret. *Cryptanalysis of $2R^-$ schemes.* Advances in Cryptology – CRYPTO 2006, Lecture Notes in Computer Science, vol. 4117, pp. 357–372, Springer–Verlag, 2006.

[15] L. Goubin, and J. Patarin. *Trapdoor One-way Permutations and Multivariate Polynomials.* Information and Communication Security, First International Conference (ICICS'97), Lecture Notes in Computer Science vol. 1334, Springer–Verlag, pp. 356–368, 1997.

[16] L. Goubin, and J. Patarin. *Asymmetric Cryptography with S-Boxes.* Information and Communication Security, First International Conference (ICICS'97), Lecture Notes in Computer Science vol. 1334, Springer–Verlag, pp. 369–380, 1997.

[17] L. Goubin, and J. Patarin. *Asymmetric Cryptography with S-Boxes – Extended Version.* Available at `http://citeseer.ist.psu.edu/patarin97asymmetric.html`.

[18] J. Gutierrez, R. Rubio, J. von zur Gathen. *Multivariate Polynomial Decomposition.* Algebra in Engineering, Communication and Computing, 14 (1), pp. 11–31.

[19] J. Gutierrez, D. Sevilla. *Computation of Unirational fields.* J. Symb. Comput. 41(11), pp. 1222–1244, 2006.

[20] J. Gutierrez, R. Rubio, D. Sevilla. *On Multivariate Rational Function Decomposition.* J. Symb. Comput. 33(5), pp. 545–562, 2002.

[21] D. Kozen, and S. Landau. *Polynomial Decomposition Algorithms.* J. Symb. Comput. (7), pp 445–456, 1989.

[22] D. Lazard. *Résolution des Systèmes d'Équations Algébriques.* Theor. Comput. Sci. (15), pages 77–110 (1981).

[23] D. Lazard. *Grbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations.* In proc. of EUROCAL '83, European Computer Algebra Conference, Lecture Notes in Computer Science vol. 162, Springer, pages 146–156 (1983).

[24] T. Matsumoto, and H. Imai. *Algebraic Methods for Constructing Asymmetric Cryptosystems.* Algebraic and Error-Correcting Codes. Prod. Third Intern. Conf., Grenoble, France, Springer-Verlag, pp. 108–119, 1985.

[25] T. Matsumoto, and H. Imai. *Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption.* Advances in Cryptology – EUROCRYPT 1988, Lecture Notes in Computer Science, vol. 330, Springer–Verlag, pp. 419–453, 1988.

[26] J. Patarin. *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88.* Advances in Cryptology – CRYPTO 1995, Lecture Notes in Computer Science, Springer-Verlag, vol. 963, pp. 248-261, 1995.

[27] M. Sweedler. *Using Groebner Bases to Determine the Algebraic and Transcendental Nature of Field Extensions: Return of the Killer Tag Variables.* Proc. AAECC, 66–75, 1993.

[28] T. Moh. *A Public Key System With Signature And Master Key Functions.* Communications in Algebra, 27(5), 2207-2222 (1999).

[29] J. von zur Gathen. *Functional decomposition of polynomials: the tame case.* J. Symb. Comput. (9), pp. 281–299, 1990.

[30] J. von zur Gathen. *Functional decomposition of polynomials: the wild case.* J. Symb. Comput. (10), pp. 437–452, 1990.

[31] D.F. Ye, K.Y. Lam, Z.D. Dai. *Cryptanalysis of "2R" Schemes*, Advances in Cryptology – CRYPTO 1999, Lecture Notes in Computer Science, vol. 1666, Springer–Verlag, pp. 315–325, 1999.

[32] D.F. Ye, Z.D. Dai and K.Y. Lam. *Decomposing Attacks on Asymmetric Cryptography Based on Mapping Compositions*, Journal of Cryptology (14), pp. 137–150, 2001.