A differential approach to polynomial equivalence problems

Abdelmejid Bayad and Ludovic Perret

April 7, 2004

Abstract

At Eurocrypt'96, J.Patarin proposed a signature and authentication scheme based on the Isomorphism of Polynomials with one Secret (IP1S) problem [P96]. Motivated by the cryptanalysis of these schemes, we propose in this paper a new efficient algorithm, outperforming all the previously known algorithms for solving the linear variant of the IP1S problem, also named Polynomial Linear Equivalence (PLE) problem in [LP].

1 Introduction

The Polynomial Linear Equivalence (PLE) problem [LP] can be outlined as follows: given multivariate polynomials $a_1(x_1,\ldots,x_n),\ldots,a_u(x_1,\ldots,x_n)$ and $b_1(x_1,\ldots,x_n),\ldots,b_u(x_1,\ldots,x_n)$ over a finite field $\mathbb{F}_q$, find - if any - an invertible matrix S with components in $\mathbb{F}_q$, such that $b_i(x_1,\ldots,x_n) = a_i((x_1,\ldots,x_n)S)$, for all $i, 1 \leq i \leq u$.

From a theoretical point of view, it has been shown in [CGP], that the PLE problem is not likely to be NP-hard. But as evidence of its hardness, it has also been proved in [CGP], that it is at least as difficult as the well known Graph Isomorphism problem.

Despite its cryptographic interest, it is only very recently that an attack against the PLE problem, better than the exhaustive search, has been designed. Indeed Geiselmann, Meier and Steinwandt in [GMS], were the first to propose an algorithm for solving this problem. Soon after, Levy-dit-Vehel and Perret proposed an improvement of this algorithm which uses Gröbner Bases [LP].

Motivated by the cryptanalysis of signature and authentication scheme whose security relies on the difficulty of the PLE problem [P96], we propose in this paper a new efficient algorithm for solving it, based on differential properties. The main advantage of this approach is to translate the PLE problem into a simple linear algebra problem.

2 Preliminaries

2.1 Notations

We introduce in this part the notations that we will use throughout this paper. We denote by $\mathbb{F}_q$ the finite field with $q = p^r$ elements (p prime, $r \geq 1$), by $\vec{x}$ the vector $(x_1,\ldots,x_n)$, by $\mathbb{F}_q[\vec{x}] = \mathbb{F}_q[x_1,\ldots,x_n]$ the polynomial ring in the n indeterminates $x_1,\ldots,x_n$ over $\mathbb{F}_q$ and $f(\vec{x})$ stands for $f(x_1,\ldots,x_n)$. Let $g(\vec{x})$ and $h_1(\vec{x}),\ldots,h_n(\vec{x})$ be polynomials. Then by $g(\vec{h}(\vec{x}))$, we shall mean the functional composition $g(h_1(\vec{x}),\ldots,h_n(\vec{x}))$ of g and the h_is.

A *monomial* is a product of a field element by a product of the variables $x_1, \ldots, x_n$. We shall define the *total degree* of a monomial $cx_1^{\mu_1} \cdots x_n^{\mu_n}$, with $c \in \mathbb{F}_q$ and $(\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$, by the sum $\sum_{i=1}^n \mu_i$. The *leading monomial* of f is the biggest monomial among the monomials of f (with respect to some admissible ordering on the monomials) and the *degree* of this polynomial is the total degree of its leading monomial. A polynomial $f \in \mathbb{F}_q[\vec{x}]$ is *homogeneous* of degree d if every monomials appearing in f has total degree d. An important fact is that every polynomial can be written uniquely as a sum of homogeneous polynomials. Namely, given $f \in \mathbb{F}_q[\vec{x}]$ then $f = \sum_d f^{(d)}$, with $f^{(d)}$ the sum of all the monomials of f of total degree d. Notice that each $f^{(d)}$ is homogeneous and we call $f^{(d)}$ the dth *homogeneous components of* f. We shall denote by $\mathcal{M}_{n,u}(\mathbb{F}_q)$ the set of $n \times u$ matrices whose components lie in $\mathbb{F}_q$, as usual, $GL_n(\mathbb{F}_q)$ denote the invertible matrices of $\mathcal{M}_{n,n}(\mathbb{F}_q)$ and $AGL_n(\mathbb{F}_q)$ denote the cartesian product $GL_n(\mathbb{F}_q) \times \mathbb{F}_q^n$. For $M \in \mathcal{M}_{n,u}(\mathbb{F}_q)$, we shall denote by $Ker_L(M) = \{\vec{x} \in \mathbb{F}_q^n : \vec{x}M = \vec{0_u}\}$ the *left kernel* of M and by $Ker_R(M) = \{\vec{x} \in \mathbb{F}_q^u : M\vec{x}^T = \vec{0_n}^T\}$ the *right kernel* of M, $\vec{0_u}$ (resp. $\vec{0_n}$) being the null vector of $\mathbb{F}_q^u$ (resp. $\mathbb{F}_q^n$).

Let $f = \sum_i a_i x^i \in \mathbb{F}_q[x]$. The *formal derivative* of f is the polynomial $\frac{df}{dx} = \sum_i i a_i x^{i-1} \in \mathbb{F}_q[x]$. More generally, when $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, the *partial derivatives* of f, denoted $\frac{\partial f}{\partial x_i}$, $1 \leq i \leq n$, are defined by considering f as a polynomial in x_i with coefficients in $\mathbb{F}_q[x_1 \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. It is not hard to verify that the $\partial/\partial x_i$'s commute with each other. Finally the *partial derivatives of order* 2 of f, denoted $\frac{\partial^2 f}{\partial x_i \partial x_j}$, $i, j, 1 \leq i, j \leq n$, are defined by $\frac{\partial^2 f}{\partial x_i \partial x_j} = \frac{\partial}{\partial x_i}\left(\frac{\partial f}{\partial x_j}\right)$. The property of the partial derivatives that we intensively use in this paper is the chain rule condition, i.e. :

$$\frac{\partial g(\vec{h})}{\partial x_i}(\vec{x}) = \sum_{j=1}^{n} \frac{\partial g}{\partial x_j}(\vec{h}(\vec{x})) \frac{\partial h_j}{\partial x_i}(\vec{x}), \text{for all } i, 1 \leq i \leq n.$$

2.2 The PLE and PAE problems

Let $\vec{a} = (a_1, \ldots, a_u)$ and $\vec{b} = (b_1, \ldots, b_u)$ be two u-tuples of polynomials over $\mathbb{F}_q[\vec{x}]$. We shall say that these polynomials are *linear-equivalent*, denoted $\vec{a} \equiv_L \vec{b}$, if there exists $S \in GL_n(\mathbb{F}_q)$ such that $b_i(\vec{x}) = a_i(\vec{x}S)$, for all $i, 1 \leq i \leq u$. We shall call such a matrix *a linear equivalence matrix between* $\vec{a}$ *and* $\vec{b}$. In the sequel, for convenience, we shall denote the equations $b_i(\vec{x}) = a_i(\vec{x}S)$, for all $i, 1 \leq i \leq u$ by $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$. The *Polynomial Linear Equivalence* (PLE) problem is then the one of finding - if any - a linear equivalence matrix between $\vec{a}$ and $\vec{b}$.
A natural extension is to consider bijective affine mappings over the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$. We shall say that two sets of polynomials $\vec{a}$ and $\vec{b}$ are *affine-equivalent*, denoted $\vec{a} \equiv_A \vec{b}$, if there exists $(S, T) \in AGL_n(\mathbb{F}_q)$ such that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S + T)$. We call such a pair *an affine equivalence pair between* $\vec{a}$ *and* $\vec{b}$, S being the *linear part* of this pair and T being its *affine part*. The *Polynomial Affine Equivalence* (PAE) problem is then the one of finding - if any - an affine equivalence pair between $\vec{a}$ and $\vec{b}$.

This last problem was first introduced in [P96] under the name *Isomorphism of Polynomials with one secret* problem, in reference to the well known graph isomorphism problem. We believe that this name is not well suited. Remember that two graphs are said to be isomorphic if and only if they are identical after a permutation of the vertices of one of the graphs. In such a setting, isomorphism is defined by a permutation and permutations are a special kind

of bijective mappings. The problems which are addressed in [P96] and here are much more general than the one of finding a permutation between two sets of polynomials. For this reason, we think that the name PLE and PAE we chose are better suited. Moreover, PLE and PAE are equivalence relations, as can be seen easily.

3 Property

3.1 Structural Properties

Let us introduce some new notations. We shall denote by $\vec{a}^{(d)} = (a_1^{(d)}, \ldots, a_u^{(d)})$ and $\vec{b}^{(d)} = (b_1^{(d)}, \ldots, b_u^{(d)})$ the dth homogeneous components of the polynomials of $\vec{a}$ and $\vec{b}$. For all $i, 1 \leq i \leq u$, $a_i^{(D_i)}$ (resp. $b_i^{(D_i)}$) denotes the monomials of highest total degree D_i of the polynomial a_i (resp. b_i). Finally, we call $\vec{a}^* = (a_1^{(D_1)}, \ldots, a_u^{(D_u)})$ and $\vec{b}^* = (b_1^{(D_1)}, \ldots, b_u^{(D_u)})$, the homogeneous components of highest total degree of the polynomials of $\vec{a}$ and $\vec{b}$. Notice that if $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, for some $S \in GL_n(\mathbb{F}_q)$, then for each $i, 1 \leq i \leq u$, a_i and b_i must have the same highest total degree D_i.

Property 1. *Let $D = max_{1 \leq i \leq u}(D_i)$. If there exists $S \in GL_n(\mathbb{F}_q)$, such that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, then:*

$$\vec{b}^{(d)}(\vec{x}) = \vec{a}^{(d)}(\vec{x}S), \textit{for all } d, 0 \leq d \leq D.$$

Proof. to complete
From this property, we deduce the two following corollaries.

Corollary 3.1. *Let A and B be the $n \times u$ matrices such that $\vec{a}^{(1)}(\vec{x}) = \vec{x}A$ and $\vec{b}^{(1)}(\vec{x}) = \vec{x}B$. If $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, for some $S \in GL_n(\mathbb{F}_q)$, then:*
i) $B = SA$,
ii) $Ker_L(A) = \big(Ker_L(B)\big)S$.

Proof. According to property 1, the fact that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, for some $S \in GL_n(\mathbb{F}_q)$, implies that $\vec{b}^{(1)}(\vec{x}) = \vec{a}^{(1)}(\vec{x}S)$, which can be rewritten as $\vec{x}B = \vec{x}SA$, i.e. $B = SA$. From this, we can now prove that $Ker_L(A) = \big(Ker_L(B)\big)S$. Indeed, let $\vec{k_a} \in Ker_L(A)$, we have $\vec{k_a}S^{-1}B = \vec{k_a}A = \vec{0_u}$, therefore $\vec{k_a}S^{-1} \in Ker_L(B)$, i.e. $\vec{k_a} \in \big(Ker_L(B)\big)S$.
Now, let $\vec{k'} = \vec{k_b}S \in \big(Ker_L(B)\big)S$, we have $\vec{0_u} = \vec{k_b}B = \vec{k'}A$ and we get that $\vec{k'}A = \vec{0_u}$, i.e. $\vec{k'} \in Ker_L(A)$. □

Corollary 3.2. *For all $i, 1 \leq i \leq u$, we denote by Q_{a_i} (resp. Q_{b_i}) the unique $n \times n$ matrix such that $\vec{a}^{(2)}(\vec{x}) = \vec{x}Q_{a_i}\vec{x}^T$ (resp. $\vec{b}^{(2)}(\vec{x}) = \vec{x}Q_{b_i}\vec{x}^T$). If there exists $S \in GL_n(\mathbb{F}_q)$, such that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, then for all $i, 1 \leq i \leq u$:*
i) $Q_{b_i} = SQ_{a_i}S^T$,
ii) $Ker_L(Q_{a_i}) = \big(Ker_L(Q_{b_i})\big)S$.

Proof. According to property 1, the fact that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)U$, for some $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, implies that $\vec{b}^{(2)}(\vec{x}) = \vec{a}^{(2)}(\vec{x}S)$. Therefore, for all $i, 1 \leq i \leq u$, we have $\vec{x}Q_{b_i}\vec{x}^T = \vec{x}SQ_{a_i}S^T\vec{x}^T$, i.e. $Q_{b_i} = SQ_{a_i}S^T$. *to complete*

Property 2. *If $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S + T)$, for some $(S, T) \in AGL_n(\mathbb{F}_q)$, then $\vec{b}^*(\vec{x}) = \vec{a}^*(\vec{x}S)$.*

Proof. The fact that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S + T)$, for some $(S,T) \in AGL_n(\mathbb{F}_q)$, implies that $\vec{b}(\vec{x} - TS^{-1}) - V = \vec{a}(\vec{x}S)$. Therefore, for each $i, 1 \leq i \leq u$, the D_ith homogeneous component of $\big(\vec{a}(\vec{x}S)\big)_i$ is equal to $\big(\vec{a}^*(\vec{x}S)\big)_i$. We conclude by noticing that the D_ith homogeneous component of $\big(\vec{b}(\vec{x} - TS^{-1})\big)_i$ is equal to $\big(\vec{b}^*(\vec{x})\big)_i$. □

The next property is an extension of a result given in [**?**].

3.2 Relations to Group theory

We investigate in this part the relations between the PLE problem and some results in group theory. Let us first recall that for all $u \geq 1$ the linear group $GL_n(\mathbb{F}_q)$ acts on the $\mathbb{F}_q[\vec{x}]$-modulus $\mathbb{F}_q[\vec{x}]^u$, through the following map:

$$\begin{array}{rccc} \phi_u : & GL_n(\mathbb{F}_q) \times \mathbb{F}_q[\vec{x}]^u & \rightarrow & \mathbb{F}_q[\vec{x}]^u \\ & (G, \vec{p}(\vec{x})) & \mapsto & p(\vec{x}S) \end{array}$$

Therefore for $p(\vec{x}) \in \mathbb{F}_q[\vec{x}]$, we shall denote by $G_{\vec{p}} = \{G \in GL_n(\mathbb{F}_q) : p_i(\vec{x}) = p_i(\vec{x}G), \forall i, 1 \leq i \leq n\}$ the *stabilizer* of $\vec{p}(\vec{x})$ (under the action of $GL_n(\mathbb{F}_q)$) and by $\mathcal{O}_{\vec{p}} = \{\vec{p}(\vec{x}G) : G \in GL_n(\mathbb{F}_q)\}$ its *orbit*. We show in this part that the the number linear equivalence matrices between $\vec{a}$ and $\vec{b}$, denoted $\mathcal{N}(\vec{a}, \vec{b})$ hereafter, is strongly related to the cardinality of the stabilizers $G_{\vec{a}}$ and $G_{\vec{b}}$.

Proposition 1. *If $G_{\vec{a}}$ is trivial and if $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, for some $S \in GL_n(\mathbb{F}_q)$, then S is unique.*

Proof. Suppose that there exists two distinct invertible matrices M and M' such that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}M)$ and $\vec{b}(\vec{x}) = \vec{a}(\vec{x}M')$. From this, we deduce that $\vec{a}(\vec{x}M) = \vec{a}(\vec{x}M')$, which implies that $\vec{a}(\vec{x}M^{-1}M') = \vec{a}(\vec{x})$ and thus $M^{-1}M'$ lies in $G_{\vec{a}}$. Since $G_{\vec{a}}$ is trivial, we get that $M^{-1}M'$ must be equal to the identity matrix $I_n \in GL_n(\mathbb{F}_q)$ and therefore $M' = M$, contradicting the assumption. □

Remark 3.1. *Since the relation $\equiv_L$ is symmetric, the conclusion of this proposition remains unchanged if we substitute $G_{\vec{a}}$ by $G_{\vec{b}}$.*

In fact, we have the more general result:

Proposition 2. *If $|G_{\vec{a}}| \leq k$, then $\mathcal{N}(\vec{a}, \vec{b}) \leq k$.*

Proof. Suppose that there exists $k+1$, 2 by 2 distinct invertible matrices $\{M_i\}_{1 \leq i \leq k+1}$ such that for all $i, 1 \leq i \leq k+1$, $\vec{b}(\vec{x}) = \vec{a}(\vec{x}M_i)$. One sees at once that for a fixed i, $\vec{a}(\vec{x}M_i) = \vec{a}(\vec{x}M_j)$ for all $j, 1 \leq j \leq k+1$. Hence, the matrices $\{M_i^{-1}M_j\}_{1 \leq j \leq k+1}$ lies in $G_{\vec{a}}$. Moreover, since the matrices $\{M_i\}_{1 \leq i \leq k+1}$ are distinct and invertible then the $k+1$ matrices $\{M_i^{-1}M_j\}_{1 \leq j \leq k+1}$ are also distinct. From this it follows that we can find two distinct indices i and j, such that $M_i^{-1}M_j = I_n$ and therefore $M_i = M_j$. Contradicting our hypothesis, since we have supposed that the matrices were distinct. □

Remark 3.2. *This proposition is also true, if we substitute $G_{\vec{a}}$ by $G_{\vec{b}}$.*

The strong relation between the linear equivalence matrices between $\vec{a}(\vec{x})$ and $\vec{b}(\vec{x})$ and theirs stabilizers:

Proposition 3. *If $\vec{a} \equiv_L \vec{b}$ then $G_{\vec{a}} = SG_{\vec{b}}S^{-1}$, for any linear equivalence matrix between $\vec{a}(\vec{x})$ and $\vec{b}(\vec{x})$.*

Proof. Since $\vec{a} \equiv_L \vec{b}$, there exists $S \in GL_n(\mathbb{F}_q)$ such that $\vec{a}(\vec{x}) = \vec{b}(\vec{x}S)$. It follows that $\vec{b}(\vec{x})$ lies on the orbit of $\vec{a}(\vec{x})$. Therefore, it is well known that the stabilizers of $\vec{a}(\vec{x})$ and $\vec{b}(\vec{x})$ are conjugate and more precisely $G_{\vec{a}} = SG_{\vec{b}}S^{-1}$.

4 Differential Properties

In the one variable case (i.e. $n = 1$), the PLE problem can be reformulated as follows: given polynomials $a_1(x), \ldots, a_u(x)$ and $b_1(x), \ldots, b_u(x)$ in $\mathbb{F}_q[x]$, find - if any - $s \in \mathbb{F}_q$, such that the equality $b_i(x) = a_i(xs)$ holds for all $i, 1 \leq i \leq u$. When computing the formal derivatives of these equalities, we get that s must be such that $\frac{db_i}{dx}(x) = s\frac{da_i}{dx}(xs)$, for all $i, 1 \leq i \leq u$. Thus, if $\frac{da_i}{dx}(0) \neq 0$, for some i, then $s = \frac{\frac{db_i}{dx}(0)}{\frac{da_i}{dx}(0)}$. In the first theorem, we show that this idea can be extended to multivariate polynomials.

Theorem 1. *If there exists $S \in GL_n(\mathbb{F}_q)$, such that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, then $J_{\vec{b}}(\vec{x}) = J_{\vec{a}}(\vec{x}S)S^t$, $J_{\vec{a}}(\vec{x}S) = \left\{\frac{\partial a_i}{\partial x_j}(\vec{x}S)\right\}_{1\leq j\leq n}^{1\leq i\leq u}$ and $J_{\vec{b}}(\vec{x}) = \left\{\frac{\partial b_i}{\partial x_j}(\vec{x})\right\}_{1\leq j\leq n}^{1\leq i\leq u}$ being the Jacobian matrices of $\vec{a}$ evaluated in $\vec{x}S$ and of $\vec{b}$ evaluated in $\vec{x}$ resp.*

Proof. Since $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, the chain rule gives that, $J_{\vec{b}}(\vec{x}) = J_{\vec{a}}(\vec{x}S)J_{\vec{x}S}(\vec{x}) = J_{\vec{a}}(\vec{x}S)S^t$. □

If we return to the one variable case, when 0 is a common zero of the polynomials $\{\frac{db_i}{dx}(x)\}_{1\leq i\leq u}$, then for solving the PLE problem, one can consider the second order (formal) derivatives. Indeed, $b_i(x) = a_i(xs)$, for all $i, 1 \leq i \leq u$, implies that $\frac{d^2b_i}{dx^2}(x) = s^2\frac{d^2a_i}{dx^2}(xs)$, for all $i, 1 \leq i \leq u$. Therefore, if $\frac{d^2a_i}{dx^2}(0) \neq 0$, for some i, then s is recovered by computing the roots of the equation $z^2\frac{d^2a_i}{dx^2}(0) - \frac{d^2a_i}{dx^2}(0) = 0$. This idea can be also adapted to the multivariate case.

Theorem 2. *If there exists $S \in GL_n(\mathbb{F}_q)$, such that $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, then:*

$$H_{b_i}(\vec{x}) = SH_{a_i}(\vec{x}S)S^t, \text{ for all } i, 1 \leq i \leq u.$$

$H_{a_i}(\vec{x}S) = \{\frac{\partial^2 a_i}{\partial x_j \partial x_k}(\vec{x}S)\}_{1\leq j,k\leq n}$ and $H_{b_i}(\vec{x}) = \{\frac{\partial^2 b_i}{\partial x_j \partial x_k}(\vec{x})\}_{1\leq j,k\leq n}$ being the Hessian matrices of a_i evaluated in $\vec{x}S$ and of b_i evaluated in $\vec{x}$ resp.

Proof. According to theorem 1, we know that if $\vec{b}(\vec{x}) = \vec{a}(\vec{x}S)$, for some $S \in GL_n(\mathbb{F}_q)$, then $J_{\vec{b}}(\vec{x})_{i,j} = \sum_{k=1}^n J_{\vec{a}}(\vec{x}S)_{i,k}s_{j,k}$, for all $i, 1 \leq i \leq u$ and for all $j, 1 \leq j \leq n$. Let $s_1, \ldots, s_n$ be the coordinate functions of $\vec{x}S$ (i.e. if $S = \{s_{i,j}\}_{1\leq i,j\leq n}$, then $s_i(\vec{x}) = \sum_{j=1}^n x_j s_{i,j}$ for all $i, 1 \leq i \leq u$). By derivating one more time, we get that for all $i, 1 \leq i \leq u$:

$$\begin{aligned} H_{b_i}(\vec{x})_{j,l} &= \frac{\partial^2 b_i}{\partial x_j \partial x_l}(\vec{x}) = \sum_{k=1}^n s_{j,k} \sum_{m=1}^n \frac{\partial^2 a_i}{\partial x_k \partial x_m}(\vec{x}S)\frac{\partial s_m}{\partial x_l}(\vec{x}) \\ H_{b_i}(\vec{x})_{j,l} &= \sum_{k=1}^n s_{j,k} \sum_{m=1}^n H_{a_i}(\vec{x}S)_{k,m}s_{l,m} = \sum_{k=1}^n s_{j,k}(H_{a_i}(\vec{x}S)S^t)_{k,l}, \text{ for all } j, l, 1 \leq j, l \leq n. \end{aligned}$$

Hence, $H_{b_i}(\vec{x}) = SH_{a_i}(\vec{x}S)S^t$, for all $i, 1 \leq i \leq u$. □

Naturally, one can also consider partial derivatives of order higher than 2. But in practice, we don't know how to use the relations given by these high order partial derivatives for our algorithm.

References

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

[CGP] Nicolas Courtois, Louis Goubin, Jacques Patarin: Improved Algorithms for Isomorphism of Polynomials. In *proc.* of Eurocrypt'1998, Springer-Verlag, pp 184-200.

[D] Matthew T. Dickerson: The Inverse of an Automorphism in Polynomial Time. Journal of Symbolic Computation 13 (1992): pp 209-220.

[G] F. R. Gantmacher: *The Theory of Matrices.* Vol. 1, Chelsea Publishing Compagny, New-York.

[GMS] Willi Geiselmann and Willi Meier and Rainer Steinwandt: An Attack on the Isomorphisms of Polynomials Problem with One Secret. Cryptology ePrint Archive: Report 2002/143.

[LP] Francoise Levy-dit-Vehel and Ludovic Perret. Polynomial equivalence problems and applications to multivariate cryptosystems. To appear in *proc.* of Indocrypt'2003.

[P96] Jacques Patarin: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms. In *proc.* of Eurocrypt'1996, Springer-Verlag, pp. 33-48.