Total Break of the ℓ-IC Signature Scheme

Pierre-Alain Fouque[1], Gilles Macario-Rat[2], Ludovic Perret[3], and Jacques Stern[1]

[1] ENS/CNRS/INRIA Pierre-Alain.Fouque@ens.fr, Jacques.Stern@ens.fr
[2] Orange Labs gilles.macariorat@orange-ftgroup.com
[3] UMPC/LIP6/SPIRAL & INRIA/SALSA ludovic.perret@lip6.fr

Abstract. In this paper, we describe efficient forgery and full-key recovery attacks on the ℓ-IC$^-$ signature scheme recently proposed at PKC 2007. This cryptosystem is a multivariate scheme based on a new internal quadratic primitive which avoids some drawbacks of previous multivariate schemes: the scheme is extremely fast since it requires one exponentiation in a finite field of medium size and the public key is shorter than in many multivariate signature schemes. Our attacks rely on the recent cryptanalytic tool developed by Dubois *et al.* against the SFLASH signature scheme. However, the final stage of the attacks require the use of Gröbner basis techniques to conclude to actually forge a signature (resp. to recover the secret key). For the forgery attack, this is due to the fact that Patarin's attack is much more difficult to mount against ℓ-IC. The key recovery attack is also very efficient since it is faster to recover equivalent secret keys than to forge.

1 Introduction

Multivariate cryptography proposes efficient cryptographic schemes well-suited for low computational devices. Since the underlying problem is not known to be easy in the quantum model, these schemes have been considered by standardization bodies as alternatives to RSA or DLog based schemes. For instance, in 2003, one promising signature scheme, called SFLASH, has been selected by the NESSIE project. SFLASH is based on the C^* cryptosystem [20] proposed by Matsumoto and Imai in 1988 and broken by Patarin in 1995 [21]. Following an idea of Shamir [25], Patarin, Goubin and Courtois proposed SFLASH [24] by removing some equations of the system. The scheme is also called C^{*-} and the generic transformation of removing equations is called the "Minus" transformation which can be applied to many multivariate schemes.

Multivariate cryptography provides public-key cryptosystems whose security is related to the problem of solving systems of quadratic or higher degree equations in many variables. This problem is known to be NP-hard and it seems to be also difficult on average. The today most efficient algorithms to solve this generic problem are Gröbner basis algorithms whose complexity is exponential[4]

[4] for systems with a finite number of solutions.

in time and space. But this general tool can perform much better in the cryptographic context since the security does not rely on hard instances. As usual in multivariate cryptography, hard instances of this NP-hard problem are hidden using linear mappings and in some cases, Gröbner basis algorithms are able to recover the hidden structure [15]. Fortunately, some countermeasures are known to avoid this kind of attack. But are there sufficient to avoid all attack ?

Recently, some breakthrough results [11, 10] have been achieved in the cryptanalysis of multivariate schemes and have lead to the efficient break of SFLASH in practice. In this work, some cryptanalytic tools have been developed which are very generic and efficient since only linear and bilinear algebra are used. They can be seen as differential cryptanalysis applied on multivariate scheme but the treatment of the differential of the public key is the main important point. The idea is to compute the differential of the public key and then to study the differential function as a bilinear function when the internal mapping is a quadratic function. The differential mapping at some point, or fix difference, is a linear map, but if we let the point to vary, we get a bilinear map. Then, in [11], the authors are able to characterize the self-adjoint operators of these bilinear functions, also called skew-symmetric linear map with respect to the bilinear function, and they show that they can be used to recover missing coordinates. For SFLASH, they show that they correspond to the conjugate by one linear and secret map of the multiplications in the extension. Finally, once all the missing equations have been recovered, Patarin's attack can be used to forge a signature for any message.

Main Results. The ℓ-IC signature scheme has been proposed by Ding, Wolf and Yang at PKC 2007. They propose a new quadratic function based on the Cremona mapping over $\mathbb{E}$, an extension of a finite field. The advantages of this function is to be more efficient to invert than SFLASH for instance, one inversion in the finite field of q^k elements, and to provide short public key. For example, the number of quadratic polynomials of the public key $\boldsymbol{P}$ is qn where n is the product of the extension field k and ℓ the number of coordinates of the Cremona map. It can be seen that the parameter k must be large enough to avoid some attack, and ℓ must be small if we want to have short public key. In general, ℓ will be equal to 3 or 5, in the parameters proposed by the authors.

In this paper, we show that the recent tools developed for SFLASH are generic and can be used to other multivariate schemes. We will use these tools to recover the missing coordinates of the ℓ-IC$^-$ scheme. Once the whole set of equations of the public key is recovered, Gröbner basis techniques can be used either to forge a signature for any message or to recover the secret key. The key recovery uses the fact that we are able to characterize and recover equivalent secret keys. More precisely, we recover two linear mappings S_0 and T_0 such that if we compose the public key $\boldsymbol{P}$ with them, $T_0^{-1} \circ \boldsymbol{P} \circ S_0^{-1}$, the new system of polynomials are equivalent to $T' \circ \boldsymbol{F} \circ S'$, where $\boldsymbol{F}$ is the central mapping and S' and T' are two linear mappings defined over the extension $\mathbb{E}$. Finally, the description of a ℓ-IC public key in $\mathbb{E}$ is easy to invert using Gröbner basis technique, since the number of unknown is small if ℓ is small.

Organization of the Paper. In Section 2, we recall some classical definitions and properties of Gröbner basis. Then, in Section 3, we describe the ℓ-IC$^-$ signature scheme. We also describe the scheme $\ell = 3$, which is the version proposed in [9]. In Section 4, we describe a special property of the differential of this new quadratic scheme. This property, together with Gröbner basis techniques, will permit us to mount an efficient forgery (Section 5) and full key recovery attacks (Section 6).

2 Gröbner Basics

We present here Gröbner basis and some of their properties. We will touch here only a restricted aspect of this theory. For a more thorough introduction to this topic, we refer the interested reader to [1, 8].

2.1 Definition – Property

We will denote by $\mathbb{K}$ a finite field of $q = p^r$ elements (p a prime, and $r \geq 1$). We shall call *ideal generated* by $p_1, \ldots, p_s \in \mathbb{K}[x_1, \ldots, x_n]$, denoted by $\langle p_1, \ldots, p_s \rangle$, the set :

$$\mathcal{I} = \langle p_1, \ldots, p_s \rangle = \left\{ \sum_{k=1}^{s} p_k u_k : u_1, \ldots, u_k \in \mathbb{K}[x_1, \ldots, x_n] \right\} \subseteq \mathbb{K}[x_1, \ldots, x_n].$$

We will denote by $V_{\mathbb{K}}(\mathcal{I}) = \left\{ \mathbf{z} \in \mathbb{F}_q^n : p_i(\mathbf{z}) = 0 \, \forall i, 1 \leq i \leq s \right\}$ the *variety associated* to $\mathcal{I}$. Gröbner bases offer an explicit method for describing varieties. Informally, a Gröbner basis of an ideal $\mathcal{I}$ is a computable generating set of $\mathcal{I}$ with "good" algorithmic properties. These bases are defined with respect to *monomial orderings*. For instance, the *lexicographical* (Lex) and *degree reverse lexicographical* (DRL) orderings – which are widely used in practice – are defined as follows:

Definition 1 *Let* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. *Then:*
– $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \succ_{\mathrm{Lex}} x_1^{\beta_1} \cdots x_n^{\beta_n}$ *if the left-most nonzero entry of* $\alpha - \beta$ *is positive.*
– $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \succ_{\mathrm{DRL}} x_1^{\beta_1} \cdots x_n^{\beta_n}$ *if* $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$, *or* $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ *and the right-most nonzero entry of* $\alpha - \beta$ *is negative.*

Once a (total) monomial ordering is fixed, we can introduce the following definitions :

Definition 2 *We shall call* total degree *of a monomial* $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ *the sum* $\sum_{i=1}^n \alpha_i$. *The* leading monomial *of* $p \in \mathbb{K}[x_1, \ldots, x_n]$ *is the largest monomial (w.r.t. some monomial ordering* $\prec$*) among the monomials of* p. *This leading monomial will be denoted by* $\mathrm{LM}(p, \prec)$. *The* degree *of* p, *denoted* $\deg(p)$, *is the total degree of* $\mathrm{LM}(p, \prec)$.

We are now in a position to define more precisely the notion of Gröbner basis.

Definition 3 *A set of polynomials $G \subset \mathbb{K}[x_1, \ldots, x_n]$ is a* Gröbner basis *– w.r.t. a monomial ordering $\prec$ – of an ideal $\mathcal{I}$ in $\mathbb{K}[x_1, \ldots, x_n]$ if, for all $p \in \mathcal{I}$, there exists $g \in G$ such that* $\mathrm{LM}(g, \prec)$ *divides* $\mathrm{LM}(p, \prec)$.

Gröbner bases computed for a lexicographical ordering (Lex-Gröbner bases) permit to easily describe varieties. A Lex-Gröbner basis of a *zero-dimensional system* (i.e. with a finite number of zeroes over the algebraic closure) is always as follows

$$\{f_1(x_1) = 0, f_2(x_1, x_2) = 0, \ldots, f_{k_2}(x_1, x_2) = 0, \ldots, f_{k_n}(x_1, \ldots, x_n)\}$$

To compute the variety, we simply have to successively eliminate variables by computing zeroes of univariate polynomials and back-substituting the results.

From a practical point of view, computing (directly) a Lex-Gröbner basis is much slower that computing a Gröbner basis w.r.t. another monomial ordering. On the other hand, it is well known that computing degree reverse lexicographical Gröbner bases (DRL-Gröbner bases) is much faster in practice. The FLGM algorithm [14] permits – in the zero-dimensional case – to efficiently solve this issue. This algorithm use the knowledge of a Gröbner basis computed for a given order to construct a Gröbner for another order. The complexity of this algorithm is polynomial in the number of solutions of the ideal considered.

DRL-Gröbner bases have another interesting property. Namely, these bases permit to recover low-degree relations between the inputs/outputs of a vectorial function $\mathbf{f} = (f_1, \ldots, f_m) : \mathbb{K}^n \to \mathbb{K}^m$.

Proposition 1. *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be polynomials of $\mathbb{K}[x_1, \ldots, x_n]$. We shall call* ideal of relations *of $\mathbf{f}$ the set :*

$$\mathcal{I}_{\mathcal{R}}(\mathbf{f}) = \big\langle z_1 - f_1(x_1, \ldots, x_n), \ldots, z_m - f_m(x_1, \ldots, x_n)\big\rangle \in \mathbb{K}[x_1, \ldots, x_n, z_1, \ldots, z_m].$$

If $\mathcal{I}_{\mathcal{R}}(\mathbf{f})$ is radical, then a DRL-Gröbner basis G (with $x_1 > \cdots > x_n > z_1 > \cdots > z_m$) of $\mathcal{I}_{\mathcal{R}}(\mathbf{f})$ describes all the (independent) algebraic relations between the inputs/outputs of $\mathbf{f}$. In particular, G contains a linear basis of the polynomials $Q \in \mathcal{I}_{\mathcal{R}}(\mathbf{f})$ s. t. :

$$\deg(Q) = \min_{P \in \mathcal{I}_{\mathcal{R}}(\mathbf{f})}\big(\deg(P)\big).$$

Note that in the cryptographic context, the ideals (of relations) are usually radicals. We can indeed always include the field equations. So, this condition is not really restrictive.

2.2 Computing Gröbner bases

The historical method for computing Gröbner bases is Buchberger's algorithm [6, 5]. Recently, more efficient algorithms have been proposed, namely the F_4 and F_5 algorithms [12, 13]. These algorithms are based on the intensive use of linear algebra techniques. Precisely, F_4 can be viewed as the "gentle" meeting of Buchberger's algorithm and Macaulay ideas [19]. In short, the arbitrary choices

– which limit the practical efficiency of Buchberger's algorithm – are replaced in F_4 by computational strategies related to classical linear algebra problems (mainly the computation of a row echelon form).

In [13], a new criterion (the so-called F_5 criterion) for detecting useless computations has been proposed. It is worth pointing out that Buchberger's algorithm spends 90% of its time to perform these useless computations. Under some regularity conditions, it has been proved that all useless computations can be avoided. A new algorithm, called F_5, has then been developed using this criterion and linear algebra methods. Briefly, F_5 constructs incrementally the following matrices in degree d :

$$A_d = \begin{array}{c} \\ t_1 f_1 \\ t_2 f_2 \\ t_3 f_3 \\ \dots \end{array} \begin{array}{c} m_1 \succ m_2 \succ m_3 \dots \\ \begin{bmatrix} \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix} \end{array}$$

where the indices of the columns are monomials sorted for the admissible ordering $\prec$ and the rows are product of some polynomials f_i by some monomials t_j such that $\deg(t_j f_i) \leq d$. For a *regular system* [13] (resp. *semi-regular system* [3, 4]) the matrices A_d are of full rank. In a second step, row echelon forms of theses matrices are computed, i.e.

$$A'_d = \begin{array}{c} \\ t_1 f_1 \\ t_2 f_2 \\ t_3 f_3 \\ \dots \end{array} \begin{array}{c} m_1\ m_2\ m_3 \dots \\ \begin{bmatrix} 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ 0 & 0 & 0 & \dots \end{bmatrix} \end{array}$$

For a sufficiently large d, A'_d contains a Gröbner basis of the considered ideal. An important parameter to evaluate the complexity of F_5 is the maximal degree d_{reg} occurring in the computation and the size $N_{d_{\mathrm{reg}}}$ of the matrix $A_{d_{\mathrm{reg}}}$. The overall cost is dominated by $N_{d_{\mathrm{reg}}}^{\omega}$, with $2 \leq \omega < 3$ denoting the linear algebra constant. Very roughly, $N_{d_{\mathrm{reg}}}$ can be approximated by $\mathcal{O}(n^{d_{\mathrm{reg}}})$ yielding to a global complexity of :

$$\mathcal{O}(n^{\omega \cdot d_{\mathrm{reg}}});$$

more details on this complexity analysis, and further complexity results, can be found in [3, 4].

To date, F_5 is the most efficient method for computing Gröbner bases, and hence zero-dimensional varieties. From a practical point of view, the gap with other algorithms computing Gröbner bases is consequent. Notably, it has been proved [2] from both a theoretical and practical point of view that XL [7] – which is an algorithm proposed by the cryptographic community for solving overdefined system of equations – is a redundant version of F_4 and less efficient than F_5.

3 The ℓ-IC$^-$ Signature Scheme

In this part, we describe the ℓ-IC$^-$ multivariate signature scheme proposed at PKC'07 by Ding, Wolf and Yang [9]. Note that our description differs from the original description given by the authors of [9]; allowing us to present our attacks in a concise way.

The design principle of ℓ-IC schemes is classical in multivariate cryptography. Namely, we start from a well chosen algebraic system $\mathbf{F}$ which is "easy" to solve, and then hide this central system using linear and invertible transformations S and T following the idea of McEliece's cryptosystem :

$$\mathbf{P} = T \circ \mathbf{F} \circ S, \tag{1}$$

For ℓ-IC, the central function $\mathbf{F}$ in $\mathbb{E}[X_1, X_2, \ldots, X_\ell]^\ell$ is obtained by considering the so called *Cremona mapping* which is defined – over an extension $\mathbb{E}$ of degree k of $\mathbb{K}$ – as follows :

$$\mathbf{F}(X_1, X_2, \ldots, X_\ell) = (X_1^{q^{\lambda_1}} X_2, X_2^{q^{\lambda_2}} X_3, \ldots, X_\ell^{q^{\lambda_\ell}} X_1). \tag{2}$$

This function can be invertible for well chosen parameters and it is efficient to invert since only one inversion in $\mathbb{E}$ is required: once X_1 is recover, only division can be used as we will see in the sequel since except λ_1, all other λ_i can be set to 0.

The public key consists in $\mathbf{P}$ and to sign a message $\boldsymbol{m}$ of n bits, we inverse it using T, we compute an inverse of $\mathbf{F}$, and finally we inverse S to find a preimage $\boldsymbol{s}$ of $\boldsymbol{m}$ for the function $\mathbf{P}$. To verify a signature $\boldsymbol{s}$, it is sufficient to evaluate the public key $\mathbf{P}$ and check that it is equal to the message $\boldsymbol{m}$.

We introduce now some notations in order to provide a compact representation of $\mathbf{F}$. We will denote by $x \otimes y$ the component-wise multiplication of $x = (x_1, x_2, \ldots, x_\ell)$ and $y = (y_1, y_2, \ldots, y_\ell)$, i.e. :

$$x \otimes y = (x_1 y_1, x_2 y_2, \ldots, x_\ell y_\ell).$$

Moreover, $\mathcal{R}$ will denote the left rotation operator, namely :

$$\mathcal{R}(x) = (x_2, x_3, \ldots, x_\ell, x_1).$$

Finally, if $\Lambda = (\lambda_1, \ldots, \lambda_\ell) \in \mathbb{N}^\ell$, then $\mathcal{E}_\Lambda$ will denote :

$$\mathcal{E}_\Lambda(x) = (x_1^{q^{\lambda_1}}, \ldots, x_\ell^{q^{\lambda_\ell}}).$$

With these notations, the central map $\mathbf{F}$ can be expressed as :

$$\mathbf{F}(x) = \mathcal{E}_\Lambda(x) \otimes \mathcal{R}(x).$$

In order to combine $\mathbf{F}$ with the two secret transformations S and T, we have to consider some canonical bijection Φ of $\mathbb{K}^{k\ell}$ onto $\mathbb{E}^\ell$. So, $\mathbf{F}$ operates on $\mathbb{E}^\ell$ and

$\Phi^{-1} \circ \mathbf{F} \circ \Phi$ operates on $\mathbb{K}^{k\ell}$. In the sequel, we may avoid the writing of Φ when the context is obvious. Hence, we can express $\mathbf{F}$ and therefore the public key $\mathbf{P}$ as a system of $n = \ell \cdot k$ polynomials of n variables over $\mathbb{K}$. Since S, T, $\mathcal{R}$, and $\mathcal{E}_\Lambda$ are $\mathbb{K}$–linear, the polynomials of $\mathbf{P}$ are quadratic over the n variables of $\mathbb{K}$. In expression (1), note that S can be seen as a change of input variables of $\mathbf{F}$, and T as a change of output variables of $\mathbf{F}$.

We now would like to consider the simplest expressions for $\mathbf{F}$. The authors of [9] remarked that it is useless to consider expression like $\mathbf{F}(x) = \mathcal{E}_{\Lambda_1}(x) \otimes \mathcal{R}\big(\mathcal{E}_{\Lambda_2}(x)\big)$. The exponentiation $\mathcal{E}_{\Lambda_2}$ would be absorbed by the external morphism S. In the same spirit, if we consider

$$\Lambda' = (\lambda_2 + \ldots + \lambda_\ell, \lambda_3 + \ldots + \lambda_\ell, \ldots, \lambda_\ell, 0),$$

$$\Lambda'' = (\lambda_1 + \ldots + \lambda_\ell, 0, \ldots, 0),$$

$$\Lambda''' = (0, \lambda_2 + \ldots + \lambda_\ell, \lambda_3 + \ldots + \lambda_\ell, \ldots, \lambda_\ell)$$

then we have the following equality:

$$\mathcal{E}_{\Lambda'}\big(\mathcal{E}_\Lambda(x) \otimes \mathcal{R}(x)\big) = \mathcal{E}_{\Lambda''}(\mathcal{E}_{\Lambda'''}(x)) \otimes \mathcal{R}\big(\mathcal{E}_{\Lambda'''}(x)\big).$$

The exponentiation $\mathcal{E}_{\Lambda'}$ would be absorbed by the external transformation T. For Λ, we can then limit the choice to vectors such as $(\lambda, 0, \ldots, 0)$. Thus, a simple expression for $\mathbf{F}$ is given a follows :

$$\mathbf{F}(X_1, X_2, \ldots, X_\ell) = (X_1^{q^\lambda} X_2, X_2 X_3, \ldots, X_\ell X_1),$$

for some integer λ.

Ding, Wolf and Yang gave explicit formulae [9] for inverting $\mathbf{F}$ when possible, since invertibility of $\mathbf{F}$ is required in the signature scheme:

- If ℓ is even, we must have $\gcd(q^\lambda - 1, q^k - 1) = 1$. Since $q - 1$ divides $q^\lambda - 1$ and $q^k - 1$, we must have $q = 2$.
- If ℓ is odd, we must have $\gcd(q^\lambda + 1, q^k - 1) = 1$. So in this second case, the choices are $\lambda = 0$ when q is even and otherwise $\lambda > 0$ and $k/\gcd(k, \lambda)$ odd (according to [11]).

Then, for a practical signature scheme, the authors of [9] have considered the effects of some known attacks and some modified versions of the main scheme ℓ-IC supposed to defeat those attacks. Particularly for ℓ even, ℓ-IC scheme is vulnerable to the UOV attack [18, 17]. So even values of ℓ should be avoid. Then, the authors suggested a modified version, the "Minus" scheme, named ℓIC$^-$. The point is to remove r polynomials among the description of $\mathbf{P}$. It increases the complexity of Patarin and Faugère-Joux attacks by a factor q^r. As a counterpart, the scheme can only be used for signature since exhaustive search is also impossible for legitimate user.

In the sequel, we will denote by $\mathbf{P}_{\mathbf{\Pi}} \in \mathbb{E}[X_1, X_2, \ldots, X_\ell]^\ell$ the corresponding truncated public key (*i.e.* the composition of $\mathbf{P}$ with a suitable projection $\mathbf{\Pi}$). Finally, the authors propose the following sets of parameters :

$\#\mathbb{K}$	ℓ	k	n	r	Security estimation
2^8	3	10	30	20	2^{80}
2^8	3	12	36	24	2^{96}
2^8	3	16	48	32	2^{128}

4 Differential and Multiplication of ℓ-IC

In this part, we present some tools adapted for the cryptanalysis of multivariate systems. We introduce the definition of the differential and we show a special property of the differential of the central map $\mathbf{F}$ of ℓ-IC. In the next section, we show that this property translated onto the public key enables to retrieve special linear applications, which beraks the "Minus" scheme of ℓIC^-.

4.1 Differential of the Public Key

For a generic application $\mathbf{F}$ in one variable, its differential $\mathbf{DF}$ is a symmetric function in two variables defined as :

$$\mathbf{DF}(\mathbf{X}, \mathbf{A}) = \mathbf{F}(\mathbf{X} + \mathbf{A}) - \mathbf{F}(\mathbf{X}) - \mathbf{F}(\mathbf{A}) + \mathbf{F}(\mathbf{0}).$$

In the case of the central map $\mathbf{F}$ of ℓ-IC, we get explicitly:

$$\mathbf{DF}(\mathbf{X}, \mathbf{A}) = \mathcal{E}_\Lambda(\mathbf{X}) \otimes \mathcal{R}(\mathbf{A}) + \mathcal{E}_\Lambda(\mathbf{A}) \otimes \mathcal{R}(\mathbf{X}).$$

Note that in this case since $\mathbf{F}$ is quadratic function, $\mathbf{DF}$ is symmetric bilinear function.

The differential $\mathbf{DP}$ of the public key $\mathbf{P}$ is also a bilinear symmetric function and is linked to the differential of the central map $\mathbf{F}$ by the following relation :

$$\mathbf{DP}(\mathbf{X}, \mathbf{A}) = T(\mathbf{DF}(S(\mathbf{X}), S(\mathbf{A}))).$$

Furthermore, the differential $\mathbf{DP}$ can be explicitly computed from the expression of the public key $\mathbf{P}$ since the differential operator operates linearly on functions and it can be easily computed on monomials.

4.2 Characteristic Properties of the Multiplications

Since $\mathcal{R}$ and $\mathcal{E}_\Lambda$ are multiplicative,*i.e.* for all $(\mathbf{X}, \mathbf{A})$, $\mathcal{R}(\mathbf{X} \otimes \mathbf{A}) = \mathcal{R}(\mathbf{X}) \otimes \mathcal{R}(\mathbf{A})$ and $\mathcal{E}_\Lambda(\mathbf{X} \otimes \mathbf{A}) = \mathcal{E}_\Lambda(\mathbf{X}) \otimes \mathcal{E}_\Lambda(\mathbf{A})$, we have the multiplicative property of the differential $\mathbf{DF}$, for all ξ, $\mathbf{X}$, $\mathbf{A}$ in $\mathbb{E}^\ell$:

$$\mathbf{DF}(\xi \otimes \mathbf{X}, \mathbf{A}) + \mathbf{DF}(\mathbf{X}, \xi \otimes \mathbf{A}) = (\mathcal{E}_\Lambda(\xi) + \mathcal{R}(\xi)) \otimes \mathbf{DF}(\mathbf{X}, \mathbf{A}) \tag{3}$$

For simplicity, we now introduce the following notations: $M_\xi(\mathbf{X}) = \xi \otimes \mathbf{X}$ the multiplication by ξ in $\mathbb{E}^\ell$ and $N_\xi = S^{-1} \circ M_\xi \circ S$ and $L(\xi) = \mathcal{E}_\Lambda(\xi) + \mathcal{R}(\xi)$.

The key idea is the following statement.

Lemma 1. *The $\mathbb{K}$-linear applications M that satisfy for all $\mathbf{X}$, $\mathbf{A}$ in $\mathbb{E}^\ell$:*

$$\mathbf{DF}(M(\mathbf{X}), \mathbf{A}) + \mathbf{DF}(\mathbf{X}, M(\mathbf{A})) = 0 \tag{4}$$

are precisely the multiplications M_ξ with ξ satisfying $L(\xi) = 0$.

Proof Due to the property (3), we first look for the linear applications M and M' that satisfy for all $\mathbf{X}$, $\mathbf{A}$ in $\mathbb{E}^\ell$:

$$\mathbf{DF}(M(\mathbf{X}), \mathbf{A}) + \mathbf{DF}(\mathbf{X}, M(\mathbf{A})) = M'(\mathbf{DF}(\mathbf{X}, \mathbf{A})). \tag{5}$$

We now express M and M' in a well chosen basis, and then we show that the coordinates of M are those of the multiplications. Indeed, any $\mathbb{K}$-linear application over $\mathbb{E}$ can be uniquely expressed as $\sum_{v=0}^{k-1} \alpha_v x^{q^v}$ with $(\alpha_0, \ldots, \alpha_{k-1})$ in $\mathbb{E}^k$. Hence, the w-th coordinate of $M(X)$ and $M'(X)$ can be expressed respectively as:

$$\sum_{u=0}^{\ell-1} \sum_{v=0}^{k-1} \alpha_{u,v,w} X_w^{q^v} \text{ and } \sum_{u=0}^{\ell-1} \sum_{v=0}^{k-1} \beta_{u,v,w} X_w^{q^v},$$

for some $\alpha_{u,v,w}$ and $\beta_{u,v,w}$ in $\mathbb{E}$. The function $\mathbf{F}$ is defined as in (2), so the w-th coordinate of $\mathbf{DF}(\mathbf{X}, \mathbf{A})$ is

$$X_w^{q^{\lambda_w}} A_{w+1} + A_w^{q^{\lambda_w}} X_{w+1}.$$

Then by considering the w-th coordinate of equation (5) we get:

$$\begin{aligned}\sum_{u=0}^{\ell-1} \sum_{v=0}^{k-1} \alpha_{u,v,w}^{q^{\lambda_w}} \left(X_u^{q^{v+\lambda_w}} A_{w+1} + A_w^{q^{v+\lambda_u}} X_{w+1} \right) + \alpha_{u,v,w+1} \left(X_u^{q^v} A_w^{\lambda_w} + A_w^{q^v} X_w^{\lambda_w} \right) \\ = \sum_{u=0}^{\ell-1} \sum_{v=0}^{k-1} \beta_{u,v,w} \left(X_u^{q^{\lambda_u}} A_{u+1} + A_u^{q^\lambda} X_{u+1} \right)^{q^v}\end{aligned} \tag{6}$$

The functions $X_a^{q^b} A_c^{q^d}$ are linearly independent. So, we can derive as many relations as the number of these functions, for each coordinate equation (6). Since one given coefficient $\alpha_{a,b,c}$ occurs at most four times in all these relations, we can see that many of them are null, since corresponding relations are trivial. Coefficients $\alpha_{u,v,w}$ appearing in non trivial relations, so that may be not null, have the following indexes: $(w, 0, w)$, $(w + 1, -\lambda_w, w)$, $(w + 2, -\lambda_w - \lambda_{w+1}, w)$, $(w + 1, 0, w + 1)$, $(w, \lambda_w, w + 1)$, $(w - 1, \lambda_w + \lambda_{w-1}, w + 1)$. At this point, we must recall that "$w + 1$" is in fact the successor of w in $(0, \ldots, \ell - 1)$ or that w are taken $\bmod \ell$. Hence we may consider that "$\ell + 1 = 1$" and "$1 - 1 = \ell$". This is why we now have to consider two cases: ($\ell = 3$, q even), and ($\ell = 3$, q odd) or $\ell \geq 5$.

- In the first case ($\ell = 3$, q even), there are two kinds of "side effect", since "$w - 1 = w + 2$" for indexes, and "$X + X = 0$" in $\mathbb{E}$. In this case, we have $\Lambda = (0, 0, 0)$, and $F(X) = X \otimes \mathcal{R}(X)$. The solutions of equation (5) are in fact the

$\mathbb{E}$-linear applications over $\mathbb{E}^\ell$. One can check easily that in this case, solutions M of equation (5) can be expressed as $\alpha \otimes X + \beta \otimes \mathcal{R}(X) + \gamma \otimes \mathcal{R}(\mathcal{R}(X))$, for some α, β, and γ in $\mathbb{E}$. Nevertheless, since in equation (4), is in fact equation (5) where $M' = 0$, the only non trivial relations are: $\alpha_{1,0,1} = \alpha_{2,0,2} = \alpha_{3,0,3}$. Hence we have $M(X) = (\alpha_{1,0,1}X_1, \alpha_{2,0,2}X_2, \alpha_{3,0,3}X_3) = (\alpha_{1,0,1}, \alpha_{2,0,2}, \alpha_{3,0,3}) \otimes X$.
- In the second case, the only non trivial relations that remain are: $\alpha_{w,0,w}^{q^{\lambda_w}} + \alpha_{w+1,0,w+1} = \beta_{w,0,w}$. Hence the result: $M(X) = \alpha \otimes X$, $M'(X) = (\mathcal{E}_\Lambda(\alpha) + \mathcal{R}(\alpha)) \otimes X$. When $M' = 0$, we must have $\mathcal{E}_\Lambda(\alpha) + \mathcal{R}(\alpha) = 0$.

□

By translating this result in the public key with the following property:

$$\mathbf{DP}(N_\xi(\mathbf{X}), \mathbf{A}) + \mathbf{DP}(\mathbf{X}, N_\xi(\mathbf{A})) = T(M_{L(\xi)}(\mathbf{DF}(S(\mathbf{X}), S(\mathbf{A})))) \qquad (7)$$

we get the next result:

Lemma 2. *The linear applications M that satisfy for all $\mathbf{X}$, $\mathbf{A}$ in $\mathbb{E}^\ell$:*

$$\mathbf{DP}(M(\mathbf{X}), \mathbf{A}) + \mathbf{DP}(\mathbf{X}, M(\mathbf{A})) = 0 \qquad (8)$$

are the "multiplications" N_ξ, i.e. the conjugates by S of the multiplications M_ξ with ξ satisfying $L(\xi) = 0$.

We emphasize here that finding the applications of the lemma 2 can be practically achieved, since it can be reduced to the resolution of a linear system.

To conclude this section, we give here the solutions of $L(\xi) = 0$. We need to show that $\xi = 0$ is not the only solution, and more precisely that there exist solutions whose coordinates are in $\mathbb{E}$ but not in $\mathbb{K}$. This result will be useful later.

Lemma 3. *The solutions of equation $L(\xi) = 0$ are*

- *When q is even, then $\lambda = 0$. The solutions satisfy $\xi_1 = \xi_2 = \ldots = \xi_\ell$. So $\xi = (\alpha, \ldots, \alpha)$ with α in $\mathbb{E}$.*
- *When q is odd, the solutions satisfy $\xi_1^{q^\lambda} + \xi_2 = \xi_2 + \xi_3 = \ldots = \xi_\ell + \xi_1 = 0$. So $\xi = (\alpha, \alpha, -\alpha, \ldots, \alpha, -\alpha)$ with α in $\mathbb{E}$ satisfying $\alpha^{q^\lambda} + \alpha = 0$. Since $\gcd(q^\lambda - 1, q^k - 1) \geq q - 1 > 1$, equation $\alpha^{q^\lambda} + \alpha = 0$ admits solutions in $\mathbb{E} \setminus \mathbb{K}$.*

5 Practical Cryptanalysis of ℓ-IC$^-$ for small ℓ

From now, we focus our attention to the practical cryptanalysis of the 3-IC$^-$ signature scheme. This is the signature scheme proposed in [9]. However, we would like to emphasize that the next attack can be easily extended to any ℓ-IC$^-$ signature scheme.

5.1 Roadmap of the Attack

The goal of the attack is to recover – from the truncated public key $\mathbf{P}_{\boldsymbol{\Pi}}$ – the equations that were removed. Namely, to recover the whole set of polynomials $\mathbf{P}$. Once these equations are recovered, the scheme is completely broken since a signature can be efficiently forged using Gröbner bases. The principle of the attack is very similar to the one described against SFLASH in [10]. First, we recover an invariant matrix N_ξ for the mapping $\mathbf{DP}$. This is done by solving a linear system generated from the (public) components of $\mathbf{DP}_{\boldsymbol{\Pi}}$ (see Section 4). This matrix will then permit to reconstruct the whole public key $\mathbf{P}$ as we describe in the sequel.

5.2 Description of the Attack

What we have to do is first finding one suitable linear application M satisfying:

$$\mathbf{DP}_{\Pi}\big(M(\mathbf{X}), \mathbf{A}\big) + \mathbf{DP}_{\Pi}\big(\mathbf{X}, M(\mathbf{A})\big) = 0.$$

If r the number of missing coordinates is not too high, all solutions are indeed “multiplications” N_ξ according to section 4.

We recall that $N_\xi = S^{-1}M_\xi S$, M_ξ being the matrix of multiplication by ξ in $\mathbb{E}^\ell$. Since we have the following relation:

$$\begin{aligned}
\mathbf{P}_{\Pi} \circ N_\xi &= \Pi \circ T \circ \mathbf{F} \circ S \circ N_\xi \\
&= \Pi \circ T \circ \mathbf{F} \circ S \circ S^{-1} \circ M_\xi \circ S \\
&= \Pi \circ T \circ \mathbf{F} \circ M_\xi \circ S \\
&= \Pi \circ T \circ M_{F(\xi)} \circ \mathbf{F} \circ S \\
&= \Pi \circ T \circ M_{F(\xi)} \circ T^{-1} \circ T \circ \mathbf{F} \circ S \\
&= \Pi \circ T \circ M_{F(\xi)} \circ T^{-1} \circ \mathbf{P},
\end{aligned}$$

by composing the public key $\mathbf{P}_{\boldsymbol{\Pi}}$ by N_ξ, we get another set of $(n-r)$ equations. We select randomly r equations among this set. It is very likely that this new set will be independent from the $(n-r)$ of P_Π. This is indeed the case if ξ does not have all its coordinates in $\mathbb{K}$ or more precisely if M_ξ is not diagonal. So, we have in some sense recovered the equations removed. We quoted below some experimental results that we obtained for ℓ-IC$^-$. We have done these experiments using the computer algebra Magma[5]. In this table, T_{rec} is the time to reconstruct the missing equations with our approach.

$\#\mathbb{K}$	ℓ	k	n	r	T_{rec}
2^8	3	10	30	20	12 s.
2^8	3	12	36	24	31 s.
2^8	3	16	48	32	2 min.
2^8	5	10	50	4	3 min
2^8	5	12	60	4	8 min.
2^8	5	16	80	4	36 min.

[5] http://magma.maths.usyd.edu.au/magma/

Equations linking input and output. It remains anyway to actually forge a signature using this additional knowledge. To this end, we can first try to mimic Patarin's attack on C*. It can be noted that Patarin's bilinear equations also exist for ℓ-IC. For instance, when $\ell = 3$, we can see that :

$$\begin{cases} Y_1 = X_1X_2 \\ Y_2 = X_2X_3 \\ Y_3 = X_3X_1 \end{cases} \qquad \text{implies} \qquad \begin{cases} X_3Y_1 = X_1Y_2 \\ X_2Y_3 = X_3Y_1 \\ X_1Y_2 = X_2Y_3 \end{cases}.$$

These are bilinear equations between the input $\mathbf{X} = (X_1, X_2, X_3)$ and output $\mathbf{Y} = (Y_1, Y_2, Y_3)$ of the function $\mathbf{F}$. However, the final bilinear equations is not independent from the two previous equations. We have then only $2k$ independent equations. In order to have enough independent equations, we can try to add :

$$Y_1Y_2 = X_1X_2^2X_3 = X_2^2Y_3.$$

This last equation permits to obtain k additional independent equations. It is not bilinear in the left hand side. But, this is not really an issue, since the right hand side is bilinear when char($\mathbb{E}$)= 2.
We mention that these equations can be recovered automatically using Gröbner bases. To do so, we consider the ideal of relations :

$$\mathcal{I}_{\mathcal{R}}(\mathbf{F}) = \left\langle Y_1 - X_1X_2, Y_2 - X_2X_3, Y_3 - X_1X_3 \right\rangle \in \mathbb{K}[X_1, X_2, X_3, Y_1, Y_2, Y_3].$$

This ideal is radical. Thus, a DRL-Gröbner basis G (with $X_1 > \cdots > X_3 > Y_1 > \cdots > Y_3$) of $\mathcal{I}_{\mathcal{R}}(\mathbf{F})$ contains a generator set of all the algebraic (independent) relations between the inputs/outputs of $\mathbf{F}$ (see Property 1). In this particular case, we obtain instantaneously (using the computer algebra system Magma) the following basis :

$$[X_1X_2 + Y_1, X_1X_3 + Y_3, X_2X_3 + Y_2, X_3Y_1 + X_2Y_3, X_1Y_2 + X_2Y_3, X_2^2Y_3 + Y_1Y_2].$$

Anyway, this approach does not permit to efficiently forge a signature. Unfortunately, if we try to reconstruct the corresponding equations from the (whole) public key $\mathbf{P}$, we need 2^{48} operations for the first set of parameters.

Signature Forgery. To conclude the attack, we will use another classical property of Gröbner basis. Once all the polynomials of $\mathbf{P}$ recovered, it is not difficult to forge a signature of a message $\boldsymbol{m} \in \mathbb{K}^n$ by computing a solution of the non-linear system :

$$\mathbf{P}(\mathbf{X}) - \boldsymbol{m}, \tag{9}$$

which can be done in practice for real sizes of the parameters. This behavior was already suspected by the authors of the scheme [9]. However, for the sake of completeness, we quoted below some experimental results that we obtained for ℓ-IC. We have done these experiments using Magma (v2.13-12) which includes a very efficient implementation of the Gröbner basis algorithm F_4.

$\#\mathbb{K}$	ℓ	k	n	d_{reg}	T
2^8	3	10	30	4	0.7 s.
2^8	3	12	36	4	2 s.
2^8	3	16	48	4	11 s.
2^8	5	10	50	4	12 s.
2^8	5	12	60	4	39 s.
2^8	5	16	80	4	209 s.

In this table, T denotes the amount of time needed to compute a solution of the system (9), for randomly chosen (non-zero) messages $\boldsymbol{m} \in \mathbb{K}^n$ (i.e. to forge a valid signature for $\boldsymbol{m}$). We mention that T is the time of computing Gröbner basis plus the time to compute the solution from this Gröbner basis. We have also reported the maximum degree d_{reg} reached during Gröbner bases computations. It appears that this degree is bounded from above by a constant (4), leading then to an experimental complexity for systems arising in ℓ-IC (ℓ odd) of :

$$\mathcal{O}(n^{4\cdot\omega}), \text{ with } 2 \leq \omega < 3 \text{ denoting the linear algebra constant.}$$

This implies that whole attack presented in this part is polynomial (in the number n of variables).

6 A Key-Recovery Attack for ℓ-IC$^-$ for small ℓ

In this part, we show that we can go one step further in the cryptanalysis of the ℓ-IC$^-$ scheme. Namely, we can recover the secret key (T, S), or at least one equivalent description, when ℓ is small. As previously, this attack will combine differential and Gröbner bases techniques. We will only consider the case q even, but once again this attack can easily be extended to other cases.

6.1 Equivalent Secret Keys

For an attacker, a total break of ℓ-IC is equivalent to finding a description of $\mathbf{P}$ such as $\mathbf{P} = T \circ \mathbf{F} \circ S$. In fact, this description is not unique. Indeed, it can be seen that there exist many equivalent keys [27]. For instance, since $M_{\mathbf{F}(\xi)} \circ \mathbf{F} = \mathbf{F} \circ M_\xi$, then $(T \circ M_{\mathbf{F}(\xi)}^{-1}, M_\xi \circ S)$ is another valid description. We notice here that M_ξ is not only $\mathbb{K}$-linear, but also $\mathbb{E}$-linear. So, more generally, we have to face the problem of finding an equivalent description (T', S') where $T^{-1} \circ T'$ and $S' \circ S^{-1}$ are $\mathbb{E}$-linear.

In the sequel, we will use the fact that a matrix of a $\mathbb{K}$-linear application which is also $\mathbb{E}$-linear can be viewed as a $k\ell \times k\ell$-matrix over $\mathbb{K}$ but also as a $\ell \times \ell$-block matrix whose blocks are multiplication by elements of $\mathbb{E}$.

6.2 Roadmap of the Attack

To recover one such equivalent secret keys, we consider that S and T can be decomposed into one $\mathbb{K}$-linear part and one $\mathbb{E}$-linear part, according to the previous subsection. In the first part of the attack, we will find the part of S and of T in $\mathbb{K}$ and then the parts in $\mathbb{E}$. To recover the part of S in $\mathbb{K}$, called S_0, we will use the invariants N_ξ that we recover using the differential of the public key. Then, once S_0 is recovered, we will find the part of T in $\mathbb{K}$, called T_0, using the differential $\mathbf{DP}$. In fact, $\mathbf{DP}$ depends linearly on S and T and if we compose $\mathbf{DP}$ by S_0^{-1}, then we are able to cancel the part of S in $\mathbf{DP}$. Using some clever ideas we are able to reconstruct some T_0. Finally, we find the part of S and T in $\mathbb{E}$ using Gröbner basis algorithms on the public equation composed on the right by S_0^{-1} and on the left by T_0^{-1}. The problem can then be described in $\mathbb{E}$ instead of $\mathbb{K}$. In such a case, we have reduced the number of variables to $2 \times \ell^2$. Due to the special form of the equations, the two sets of variables are separated, Gröbner basis algorithms are very efficient.

6.3 Description of the Attack

Resolution of S_0. We suppose that we have already recovered the multiplication matrix N_ξ (we have then all the polynomials of $\mathbf{P}$). We recall that:

$$SN_\xi = M_\xi S,$$

M_ξ being a block-diagonal matrix and since $\xi = (\alpha, \alpha, \alpha)$, each block of the diagonal corresponds to the same multiplication matrix by α element of $\mathbb{E}$. Our goal is to recover S from this equality.

To this end, we try to find M_ξ. Observe that α is an element of the multiplicative group $\mathbb{E}^*$ of $\mathbb{E}$. We know that $\mathbb{E}^*$ is of order $q^k - 1$. Due to the choice of the parameters, we can isolate a small subgroup of $\mathbb{E}^*$, not totally included in $\mathbb{K}^*$. Note that elements of $\mathbb{K}$ must be avoided, otherwise M_ξ would be totally diagonal, leading then to linearly dependent equations.

In our example, $q = 256$ and $k = 10, 12, 16$. Since k is even, a good candidate for the order is $o = q + 1$, but any smaller value prime with $q - 1$ will be possible. Consequently, by raising N_ξ to the power $a = (q^k - 1)/o$ we get :

$$N_\xi^a = S^{-1} M_\xi^a S = S^{-1} M_\xi^a S,$$

and ξ^a is of order o. Finally, we can test all elements ρ of order o. For each of them, we try to solve :

$$XN_\xi^a = M_\rho X.$$

Let's suppose that X_1 and X_2 are two particular invertible solutions of this equation. Then $Y = X_1 X_2^{-1}$ must satisfy the equation :

$$YM_\rho = M_\rho Y.$$

So, at this step, the solutions for S form the right coset of any particular solution and the subgroup of ℓ-by-ℓ block-matrices of elements of $\mathbb{K}$, which precisely commute with M_ρ. These are exactly the $\mathbb{E}$-linear applications. So, we can pick at random some invertible solution S_0.

Resolution of T_0. Next step is to obtain a similar description for T. We would like to gain some information on T from the differential of the public key using linear algebra. We recall that :

$$\mathbf{DP}(\mathbf{X}, \mathbf{A}) = T(\mathbf{DF}(S(\mathbf{X}), S(\mathbf{A}))).$$

From now, it will be easier to fix the first variable and to see $\mathbf{DP}_{\mathbf{X}}(\mathbf{A})$ as a linear mapping or equivalently as a matrix. So let's consider v_1 a fixed random vector. Then, consider the expression :

$$\mathbf{DP}_{v_1} \circ S_0^{-1} = T \circ \mathbf{DF}_{S(v_1)} \circ S \circ S_0^{-1}.$$

It is important to note that $\mathbf{DF}_{S(v_1)} \circ S \circ S_0^{-1}$ is actually $\mathbb{E}$-linear, not only $\mathbb{K}$-linear. The matrix $\mathbf{DP}_{v_1} \circ S_0^{-1}$ is therefore the product of T and an unknown ℓ-by-ℓ block-matrix of elements of $\mathbb{E}$. Unfortunately, this matrix is not invertible due to the underlying structure of $\mathbf{DF}$. However, this issue can be easily resolved by picking at random a second vector v_2 and some matrix R with ℓ-by-ℓ block-multiplications (i.e. R is $\mathbb{E}$-linear) and computing the matrix $\mathbf{DP}_{v_1} \circ S_0^{-1} + \mathbf{DP}_{v_2} \circ S_0^{-1} \circ R$. All possible results can be seen as a left coset which contains the real value of T. So, it suffices to pick any value T_0, provided it is invertible.

Resolution of T' and S'. In the last step, we compose the public equations on the right by S_0^{-1} and on the left by T_0^{-1}, the result is public equations expressed in $\mathbb{E}$ instead of $\mathbb{K}$. As explained in [16], we can recover the components of T' and S' by solving an algebraic system of equations. In our case, we have reduced the number of variables to $2 \times \ell^2$. This is due to the fact we are working over $\mathbb{E}$ instead of $\mathbb{K}$. Here, the number of unknowns is very small (2×3^2, for the parameters considerd). The last unknown parameters can easily be retrieved (within a second) using Gröbner bases techniques, as illustrated in the table below :

$\#\mathbb{K}$	ℓ	k	n	T
2^8	3	10	30	0.1 s.
2^8	3	12	36	0.1 s.
2^8	3	16	48	0.1 s.
2^8	5	10	50	0.3 s.
2^8	5	12	60	0.3 s.
2^8	5	16	80	0.3 s.

7 Conclusion

We have presented a forgery attack and a key recovery attack on the parameters of the ℓ-IC$^-$ signature scheme proposed in the original paper. We also shortly discuss that this attack can be extended to all other choices of parameters. The main worry when proposing a multivariate scheme is that the Minus Transformation can be used with attention now, due to the differential attack. Finally, for this scheme and contrary to the SFLASH signature scheme, we show that it is possible to recover the secret keys S and T.

Acknowledgements

The work described in this paper has been supported by the ANR MAC project and by the European Commission through the IST Program under contract IST-2002-507932 ECRYPT.

References

1. W.W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases.*, volume 3 of *Graduate Studies in Mathematics.* AMS, 1994.
2. G. Ars, J.-C. Faugère, H. Imai, M. Kawazoe, and M. Sugita. Comparison Between XL and Gröbner Basis Algorithms. In *Asiacrypt' 04*, volume 3329 of *Lecture Notes in Computer Science*, pages 338–353. Springer-Verlag, 2004.
3. M. Bardet. *Étude des Systèmes Algébriques Surdéterminés. Applications aux Codes Correcteurs et à la Cryptographie.* PhD thesis, Université de Paris VI, 2004. Thèse de Doctorat.
4. 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'05, Eighth International Symposium on Effective Methods in Algebraic Geometry*, 2005.
5. B. Buchberger. *Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory.* Recent trends in multidimensional systems theory. Reider ed. Bose, 1985.
6. B. Buchberger, G.-E. Collins, and R. Loos. *Computer Algebra Symbolic and Algebraic Computation.* Springer-Verlag, 1992. Second Edition.
7. N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In *Eurocrypt' 00*, volume 1807 of *Lecture Notes in Computer Science*, pages 392–407. Springer-Verlag, 2000.
8. D.A. Cox, J.B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: an Introduction to Computational Algebraix Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer-Verlag, 1992.
9. J. Ding, C. Wolf, and B.-Y. Yang. ℓ-Invertible Cycles for Multivariate Quadratic Public Key Cryptography. In *PKC '07*, volume 4450 of *Lecture Notes in Computer Science*, pages 266–281. Springer-Verlag, 2007.
10. V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern. Practical Cryptanalysis of SFLASH. In *Crypto '07*, volume 4622 of *Lecture Notes in Computer Science.* Springer-Verlag, 2007.
11. V. Dubois, P.-A. Fouque, and J. Stern. Cryptanalysis of SFLASH with Slightly Modified Parameters. In *Eurocrypt '07*, volume 4515 of *Lecture Notes in Computer Science*, pages 264–275. Springer-Verlag, 2007.
12. J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner Basis: F_4. *Journal of Pure and Applied Algebra*, 139:61–68, 1999.
13. J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner Basis without Reduction to Zero: F_5. In *ISSAC*, pages 75–81. ACM Press, 2002.
14. 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):329–344, 1993.
15. J.-C. Faugère and A. Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases. In *Crypto' 03*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer-Verlag, 2003.

16. J.-C. Faugère and L. Perret. Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects. In *Eurocrypt' 06*, volume 4004 of *Lecture Notes in Computer Science*, pages 30–47. Springer-Verlag, 2006.
17. A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar Signature Schemes. In *Eurocrypt' 99*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer-Verlag, 1999.
18. A. Kipnis and A. Shamir. Cryptanalysis of the Oil & Vinegar Signature Scheme. In *Crypto' 98*, volume 1462 of *Lecture Notes in Computer Science*, pages 257–266. Springer-Verlag, 1998.
19. F.S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge University Press, 1916.
20. T. Matsumoto and H. Imai. Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In *Eurocrypt '88*, volume 330 of *Lecture Notes in Computer Science*, pages 419–453. Springer-Verlag, 1988.
21. J. Patarin. Cryptoanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In *Crypto '95*, volume 963 of *Lecture Notes in Computer Science*, pages 248–261. Springer-Verlag, 1995.
22. J. Patarin. Asymmetric Cryptography with a Hidden Monomial. In *Crypto '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 45–60. Springer-Verlag, 1996.
23. J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *Eurocrypt '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer-Verlag, 1996.
24. J. Patarin, N. Courtois, and L. Goubin. FLASH, a Fast Multivariate Signature Algorithm. In *CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 298–307. Springer-Verlag, 2001.
25. A. Shamir. Efficient Signature Schemes Based on Birational Permutations. In *Crypto '93*, volume 773 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, 1993.
26. P.W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Computing*, 26:1484–1509, 1997.
27. C. Wolf and B. Preneel. Equivalent Keys in HFE, C^*, and Variations. In *Mycrypt '05*, volume 3715 of *Lecture Notes in Computer Science*, pages 33–49. Springer-Verlag, 2005.
28. C. Wolf and B. Preneel. Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations. Cryptology ePrint Archive, Report 2005/077, 2005. `http://eprint.iacr.org/`.