On Polynomial Systems
Arising from a Weil Descent

Christophe Petit[*] and Jean-Jacques Quisquater[**]

UCL Crypto Group,
Université catholique de Louvain
Place du Levant 3
1348 Louvain-la-Neuve (Belgium)
christophe.petit@uclouvain.be, jjq@uclouvain.be

Abstract. In the last two decades, many computational problems arising in cryptography have been successfully reduced to various systems of polynomial equations. In this paper, we revisit a class of polynomial systems introduced by Faugère, Perret, Petit and Renault. Based on new experimental results and heuristic evidence, we conjecture that their degrees of regularity are only slightly larger than the original degrees of the equations, resulting in a very low complexity compared to generic systems. We then revisit the application of these systems to the elliptic curve discrete logarithm problem (ECDLP) for binary curves. Our heuristic analysis suggests that an index calculus variant due to Diem requires a *subexponential* number of bit operations $O(2^{c\,n^{2/3}\log n})$ over the binary field $\mathbb{F}_{2^n}$, where c is a constant smaller than 2. According to our estimations, generic discrete logarithm methods are outperformed for any $n > N$ where $N \approx 2000$, but elliptic curves of currently recommended key sizes ($n \approx 160$) are not immediately threatened. The analysis can be easily generalized to other extension fields.

1 Introduction

While linear systems of equations can be efficiently solved with Gaussian elimination, polynomial systems are much harder to solve in general. After their introduction by Buchberger [13], Gröbner bases have become the most popular way to solve polynomial systems of equations, in particular since the development of fast algorithms like F_4 [26] and F_5 [27]. Polynomial systems arising in cryptography tend to have a special structure that simplifies their resolution. In the last twenty years, many cryptographic challenges have been first reduced to polynomial systems of equations

---

and then solved with fast and sometimes *dedicated* Gröbner basis algorithms [42,30,38,10,22,23,32,12,31].

Our contribution

In this paper, we revisit a particular class of polynomial systems introduced by Faugère et al. [33,34]. These systems naturally arise by deploying a multivariate polynomial equation over an extension field into a system of polynomial equations over the ground prime field (a technique commonly called *Weil descent*).

We first observe that polynomial systems arising from a Weil descent are a natural generalization of a well-known family of polynomial systems appearing in the cryptanalysis of HFE [48,42,18,30,38,24,10,22,23]. Starting from this observation, we extend various experimental and theoretical results on HFE to the more general class of polynomial systems arising from a Weil descent. Our results suggest that the degrees of regularity of these systems are only sligthly larger than the degrees of their equations, essentially as small as they could be.

Following [34], we subsequently study an elliptic curve discrete logarithm algorithm of Diem [21] in the case of binary fields. Based on our heuristic analysis of polynomial systems arising from a Weil descent, we conjecture that the elliptic curve discrete logarithm problem can be solved over the binary field $\mathbb{F}_{2^n}$ in *subexponential time* $O(2^{c\, n^{2/3} \log n})$, where c is a constant smaller than 2. For n prime, this problem was previously thought to have complexity $O(2^{n/2})$.

Our analysis of polynomial systems arising from a Weil descent can also be applied to the factorization problem in $SL(2, \mathbb{F}_{2^n})$, to HFE and to other discrete logarithm problems. These applications will be discussed in an extended version of this paper [49]. Although we focus on characteristic 2 in this paper, most of our results can be easily extended to other characteristics.

Outline

The remaining of this paper is organized as follows. Section 2 contains most of the notations and definitions used in the paper. Section 3 provides general background on algebraic cryptanalysis with Gröbner bases. Section 4 contains our new analysis of polynomial systems arising from a Weil descent. The application to Diem's algorithm is detailed in Section 5 and Section 6 concludes the paper.

2 Definitions and notations

We mostly follow the notations introduced in [33]. For any "small" prime p and any $n \in \mathbb{Z}$, we write $\mathbb{F}_{p^n}$ for the finite field with p^n elements. We see the field $\mathbb{F}_{p^n}$ as an n-dimensional vector space over $\mathbb{F}_p$ and we let $\{\theta_1, \ldots, \theta_n\}$ be a basis for $\mathbb{F}_{p^n}/\mathbb{F}_p$. With some abuse of notations, we use bold letters for all elements, variables and polynomials over $\mathbb{F}_{p^n}$ and normal letters for all elements, variables and polynomials over $\mathbb{F}_p$. If $x_1, \ldots, x_N$ are variables defined over a field $\mathbb{K}$, we write $R := \mathbb{K}[x_1, \ldots, x_N]$ for the ring of polynomials in these variables. Given a set of polynomials $f_1, \ldots, f_\ell \in R$, the *ideal* $I(f_1, \ldots, f_\ell) \subset R$ is the set of polynomials $\sum_{i=1}^{\ell} g_i f_i$, where, $g_1, \ldots, g_\ell \in R$. We write $\mathrm{Res}_{x_i}(f_1, f_2)$ for the *resultant* of $f_1, f_2 \in R$ with respect to the variable x_i. A *monomial* of R is a power product $\prod_{i=1}^{k} x_i^{e_i}$ where $e_i \in \mathbb{N}$. A *monomial ordering* for R is an ordering $>$ such that $m_1 > m_2 \Rightarrow m_1 m_3 > m_2 m_3$ for any monomials m_1, m_2, m_3 and $m > 1$ for any monomial m. The *leading monomial* $LM(f)$ of a polynomial $f \in R$ for a given ordering is equal to its largest monomial according to the ordering. Its *leading term* is the corresponding term. For any polynomial $f \in R$, we denote the set of monomials of f by $\mathtt{Mon}(f)$. We measure the memory and time complexities of algorithms by respectively the number of bits and bit operations required. Actual experimental results are given in megabytes and seconds. We write O for the "big O" notation: given two functions f and g of n, we say that $f = O(g)$ if there exist $N, c \in \mathbb{Z}^+$ such that $n > N \Rightarrow f(n) \le cg(n)$. Similarly, we write o for the "small o" notation: given two functions f and g of n, we say that $f = o(g)$ if for any $\epsilon > 0$, there exists $N \in \mathbb{Z}$ such that for any $n > N$, we have $|f(n)| \le \epsilon |g(n)|$. Finally, we write ω for the *linear algebra constant*. Depending on the algorithm used for linear algebra, we have $2.376 \le \omega \le 3$.

3 Background on polynomial system resolution

Let R be a polynomial ring and let $>$ be a fixed monomial ordering for this ring. A *Gröbner basis* [13,19] of an ideal $I(f_1, \ldots f_\ell) \subset R$ is a basis $\{f_1', \ldots, f_{\ell'}'\}$ of this ideal such that for any $f \in I(f_1, \ldots f_\ell)$, there exists $i \in \{1, \ldots, \ell'\}$ such that $\mathrm{LT}(f_i')|\mathrm{LT}(f)$. The first Gröbner basis algorithm was provided by Buchberger in his PhD thesis [13]. Lazard [44] later observed that computing a Gröbner basis is essentially equivalent to performing linear algebra on *Macaulay matrices* at a certain degree.

Definition 1 (Macaulay Matrix [45,46]). *Let R be a polynomial ring over a field K and let $\mathcal{B}_d := \{m_1 > m_2 > \cdots\}$ be the sorted set of*

all monomials of degree $\leq d$ for a fixed monomial ordering. Let $F :=$ $\{f_1, \ldots, f_\ell\} \subset R$ be a set of polynomials of degrees $\leq d$. For any $f_i \in F$ and $t_j \in \mathcal{B}_d$ such that $\deg(f_i) + \deg(t_j) \leq d$, let $g_{i,j} := t_j f_i$ and let $c_{i,j}^k \in K$ be such that $g_{i,j} = \sum_{m_k \in \mathcal{B}} c_{i,j}^k m_k$. The Macaulay matrix $\mathcal{M}_d(F)$ *of degree d is a matrix containing all the coefficients $c_{i,j}^k$, such that each row corresponds to one polynomial $g_{i,j}$ and each column to one monomial $m_k \in \mathcal{B}_d$.*

The idea behind Lazard's observation is *linearization*: new equations for the ideal are constructed by algebraic combinations of the original equations, every monomial term appearing in the new equations is treated as an independent new variable, and the system is solved with linear algebra. Gröbner basis algorithms like F_4 [26] and F_5 [27] successively construct Macaulay matrices of increasing sizes and remove linear dependencies in the rows until a Gröbner basis is found. Moreover, they optimize the computation by avoiding monomials t_j that would produce trivial linear combinations such as $f_1 f_2 - f_2 f_1 = 0$. The complexity of this strategy is determined by the cost of linear algebra on the largest Macaulay matrix occuring in the computation.

The degree of the largest Macaulay matrix appearing in a Gröbner basis computation with the algorithm F5 is called the *degree of regularity D_{reg}*. For a "generic" sequence of polynomials $f_1, \ldots, f_\ell \in R$ (with $\ell \leq n$), this degree is equal to $1 + \sum_{i=1}^{\ell}(\deg(f_i) - 1)$ [6]. The degree of regularity can be precisely estimated in the case of *regular* and *semi-regular* sequences [6,8] and (assuming a variant of Fröberg conjecture) in a few other cases [28,11]. However, precisely estimating this value for other classes of systems (in particular for the various structured systems appearing in cryptanalysis problems) may be a very difficult task. In practice, the degree of regularity may often be approximated by the first degree at which a non trivial *degree fall* occurs during a Gröbner basis computation.

Definition 2. *Let R be a polynomial ring over a field K and let $F :=$ $\{f_1, \ldots, f_\ell\} \subset R$. The* first fall degree *of F is the smallest degree $D_{firstfall}$ such that there exist polynomials $g_i \in R$ with $\max_i(\deg(f_i) + \deg(g_i)) = D_{firstfall}$, satisfying $\deg(\sum_{i=1}^{\ell} g_i f_i) < D_{firstfall}$ but $\sum_{i=1}^{\ell} g_i f_i \neq 0$.*

We have $D_{reg} \geq D_{firstfall}$. For many classes of polynomial systems, the two definitions lead to very close numbers. Although this is not true in general (counter-examples can be easily produced), it seems to be true for "random systems" and "most real-life systems of equations" [38, p. 350] including HFE and its variants [30,38,24,22,23,11]. This can intuitively be

explained by the observation that an extremely large number of relations with a degree fall occur at the degree $D_{firstfall}$ or the degree $D_{firstfall}+1$ in these contexts, and these low degree relations can in turn be combined to produce lower degree relations [24, p. 561], until a Gröbner basis is finally found. In fact, the *first fall degree* has even sometimes been called *degree of regularity* in the cryptography community [24,22,23].

Many polynomial systems arising in cryptanalysis are very far from generic ones. In fact, their special structures often induce lower degrees of regularity, hence much better time complexities. Gröbner basis techniques have successfully attacked many cryptosystems, including HFE and its variants [48,42,30,38,10,22,23], the Isomorphism of Polynomials [32,12] and some McEliece variants [31]. In many cases, the resolution of these systems could be accelerated using *dedicated* Gröbner basis algorithms that exploited the particular structures. As was first pointed out in [33,34], this is also the case for polynomial systems arising from a Weil descent.

4   Polynomial systems arising from a Weil descent

Let n, n', m be positive integers and let V be a vector subspace of $\mathbb{F}_{2^n}/\mathbb{F}_2$ with dimension n'. Let $\mathbf{f} \in \mathbb{F}_{2^n}[\mathbf{x_1}, \dots, \mathbf{x_m}]$ be a multivariate polynomial with degrees bounded by $2^t - 1$ with respect to all variables. In [33,34], Faugère et al. considered the following problem:

$$\text{Find } \mathbf{x_i} \in V, i = 1, \dots, m, \text{ such that } \mathbf{f}(\mathbf{x_1}, \dots, \mathbf{x_m}) = \mathbf{0}. \qquad (1)$$

The constraints $\mathbf{x_i} \in V, i = 1, \dots, m$ are called *linear constraints*. From now on, we assume that $mn' \approx n$ such that Problem (1) has about one solution on average. We also assume $n' \geq t$. The *multilinear* case ($t = 1$) was first considered in [33] and later extended in [34].

Following [33,34], Problem (1) can be reduced to a system of polynomial equations. Let $\{\theta_1, \dots, \theta_n\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and let $\{\mathbf{v_i}|i = 1, \dots, n'\}$ be a basis of V over $\mathbb{F}_2$. We define $m \cdot n'$ variables x_{ij} over $\mathbb{F}_2$ such that $\mathbf{x_i} = \sum_{j=1}^{n'} x_{ij}\mathbf{v_j}$ and we group them into m *blocks of variables* $X_i := \{x_{ij}|j = 1, \dots, n'\}$. By substituting each $\mathbf{x_i}$ in $\mathbf{f}$, decomposing in the basis $\{\theta_1, \dots, \theta_n\}$ and reducing by the *field equations* $x_{ij}^2 - x_{ij} = 0$, we obtain $\mathbf{0} = \mathbf{f}(\mathbf{x_1}, \dots, \mathbf{x_m}) = \mathbf{f}\left(\sum_{j=1}^{n'} x_{1j}\mathbf{v_j}, \dots, \sum_{j=1}^{n'} x_{mj}\mathbf{v_j}\right) = [\mathbf{f}]_1^{\downarrow}\theta_1 + \dots + [\mathbf{f}]_n^{\downarrow}\theta_n$ for some $[\mathbf{f}]_1^{\downarrow}, \dots, [\mathbf{f}]_n^{\downarrow} \in \mathbb{F}_2[x_{11}, \dots, x_{mn'}]$ that depend on $\mathbf{f}$ and on the vector subspace V. Problem (1) can therefore be reformulated as finding a solution to the (algebraic) system

$$[\mathbf{f}]_1^{\downarrow} = 0, \dots, [\mathbf{f}]_n^{\downarrow} = 0. \qquad (2)$$

Due to the bounds on the degrees of $\mathbf{f}$, this system has a *block structure*: the degrees of all polynomials $[\mathbf{f}]_k^{\downarrow}$ are bounded by t with respect to all blocks of variables. The resolution of System (2) can therefore be greatly accelerated using *block-structured* Gröbner basis algorithms [29,33,34].

Link to HFE In this paper, we observe that a particular instance of Problem (1) had previously been studied in the cryptography literature. Indeed, the well-known problem of inverting HFE [48,30,38] leads to a particular instance of System (2), where the polynomial $\mathbf{f}$ is univariate ($m = 1$) and the linear constraints are trivial ($V = \mathbb{F}_{2^n}$).[1] Interestingly, although the polynomial $\mathbf{f}$ used in HFE has a particular shape (it leads to quadratic equations over $\mathbb{F}_2$), we will see that this shape has generically little influence on the complexity of Problem (1).

Ten years of research on HFE systems have shown that their degrees of regularity are abnormally low compared to generic systems, resulting in very efficient attacks. Although no definitive proof of these results has been published yet, the experimental observations of [30] are now being supported by theoretical evidence such as the isolation of a subsystem with less variables [38], the existence of many low degree equations [17], first fall degree computations [22,24] and complexity results on the MinRank problem [11]. In this paper, we generalize some of these results to polynomial systems arising from a Weil descent.

Experimental observations We start our analysis of these systems with an experimental study of their degree of regularity for various parameters n, m, n', t. For each set of parameters, we generate a random vector space V of dimension n' and a random multivariate polynomial $\mathbf{f}(\mathbf{x_1}, \ldots, \mathbf{x_m})$ with degree bounded by $2^t - 1$ with respect to each variable. We then perform a Weil descent on this polynomial and we append the field equations to the system. Finally, we apply the Magma function *Groebner* to the result and we collect the maximal degree D reached during the computation, as given by the *Verbose* output of the Magma function. We repeat each experiment 100 times.

Table 1 reports the average value of D for these experiments, as well as the average computation time and the maximal memory used (all experiments were done on an Intel Xeon CPU X5500 processor running at 2.67

---

[1] In HFE contexts, the attacker is not given $\mathbf{f}$ but only a "hidden" version of System (2). This can be ignored in the complexity analysis of Gröbner basis algorithms since the hiding transformation only consists of a linear combinations of the equations and a linear change of variables [48,38].

Table 1: Average maximal degree reached in Gröbner Basis experiments, average computation time (in seconds) and maximal memory requirements (in MB) for random polynomials

t	n	n'	m	$mt+1$	D_{av}	Time	Mem.	t	n	n'	m	$mt+1$	D_{av}	Time	Mem.
1	6	3	2	3	3.1	0	10	2	6	3	2	5	5.1	0	10
1	6	2	3	4	3.8	0	10	2	6	2	3	7	6.7	0	10
1	8	4	2	3	3.0	0	11	2	8	4	2	5	5.1	0	11
1	12	6	2	3	3.6	0	11	2	9	3	3	7	7.2	0	12
1	12	4	3	4	4.2	0	11	2	12	4	3	7	7.1	1	38
1	12	3	4	5	5.3	0	14	2	12	3	4	9	9.3	2	95
1	12	2	6	7	7.4	1	23	2	15	5	3	7	7.0	12	263
1	15	5	3	4	4.1	5	20	2	16	8	2	5	5.1	13	36
1	15	3	5	6	6.3	7	114	3	6	3	2	7	6.6	0	10
1	16	8	2	3	3.0	14	25	3	12	6	2	7	7.0	1	31
1	16	4	4	5	5.3	16	98	3	12	4	3	10	10.1	9	70
1	16	2	8	9	9.6	69	3388	3	12	3	4	13	12.6	70	113
1	18	9	2	3	3.0	85	74	3	15	5	3	10	10.0	118	2371
1	18	6	3	4	4.1	86	89	3	16	8	2	7	7.0	23	253
1	18	3	6	7	7.4	233	5398	3	16	4	4	13	13.2	1891	20135
1	20	10	2	3	3.0	487	291	4	8	4	2	9	8.7	1	11
1	20	5	4	5	6.2	515	733	4	12	4	3	13	12.6	199	116
1	20	4	5	6	6.2	669	3226	4	15	5	3	13	13.1	2904	6696

GHz, with 24 GB RAM). As is often the case in Gröbner basis computations, our experiments were limited more by the memory requirements than by the computation time.

For all parameter sets, the maximal degrees occuring during Gröbner basis computations were much smaller than the degrees of regularity of regular or semi-regular systems with the same degrees. In fact, our experiments suggest that the degree of regularity of System (2) is not much higher than the value $mt+1$. In other words since the original equations have degree mt, the degree of regularity is essentially as small as it could be. The even lower values obtained for all parameter sets such that $t = n'$ can be explained by a probable degeneracy in the degrees of the equations. Taking $m = 1$, we recover known experimental results on HFE [30].

Heuristic upper bound on D_{reg} As a first step towards explaining these experimental results, we follow Granboulan et al. [38] and we bound of the degree of regularity of System (2) from above by the degree of regularity of a smaller system with a lower number of variables. We now suppose that $\{\theta_1, \ldots, \theta_n\}$ is a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, such that $\theta_i := \theta^{2^{i-1}}$ for some $\theta \in \mathbb{F}_{2^n}$. Let $v_{ij} \in \mathbb{F}_2$ such that $\mathbf{v_i} = \sum_{j=1}^{n} v_{ij}\theta_j$.

We define nm auxiliary binary variables y_{ij} such that $\mathbf{x_i} = \sum_{j=1}^n y_{ij}\theta_j$. Proceeding to a Weil descent as above, we obtain a new system[2]

$$[\mathbf{f}]_1^{\downarrow y} = 0, \ldots, [\mathbf{f}]_n^{\downarrow y} = 0 \tag{3}$$

in the variables y_{ij}, to which we add $m(n+n')$ field equations $y_{ij}^2 - y_{ij} = 0$ and $x_{ij}^2 - x_{ij} = 0$, as well as mn linear equations $y_{ij} = \sum_{k=1}^n x_{ik}v_{kj}$ modeling the linear constraints. The resulting system of $m(n+n')$ variables and $n + m(n+n') + mn$ equations is equivalent to System (2) (with the field equations), hence they have the same degree of regularity.

Following Granboulan et al. [38], we perform additional modifications on this system to obtain a new system with less variables and higher or equal degree of regularity. First, we observe that linear equations do not contribute to the degree of regularity and can therefore be removed without affecting it. The resulting system is composed of $n+mn$ equations containing only the variables y_{ij} and mn' field equations $x_{ij}^2 - x_{ij} = 0$. Without decreasing the degree of regularity, we can focus on the first part containing Equations (3) and the field equations $y_{ij}^2 - y_{ij} = 0$.

In the next step, we observe that the degree of regularity of this system is not affected if we see the variables y_{ij} over $\mathbb{F}_{2^n}$ rather than over $\mathbb{F}_2$. Thanks to the field equations, the set of solutions is not affected by this change either. We then apply an invertible linear transformation on Equations (3), defined by $F_i := \sum_{j=1}^n \theta^{2^{i+j}} [\mathbf{f}]_j^{\downarrow y}$ for $i = 1, \cdots, n$. This transformation implies $F_i = F_1^{2^{i-1}}$. Finally, we perform a linear change of variables defined by $z_{ij} := \sum_{k=1}^n \theta^{2^{j+k-1}} y_{ik}$ for $i = 1, \ldots, m$, and $j = 1, \cdots, n$. Since this corresponds to setting $z_{i1} = \mathbf{x_i}$, $z_{i2} = \mathbf{x_i}^2$, $\ldots, z_{i,n} = \mathbf{x_i}^{2^{n-1}}$, each F_k only depends (linearly) on z_{ij}, $k \leq j \leq t+k-1$. A last linear transformation changes the field equations into $z_{ij}^2 = z_{i,j+1}$ and $z_{i,n}^2 = z_{i,1}$.

Since $F_2 = F_1 \cdot F_1$ modulo the field equations, the polynomial F_2 can be expressed at the degree $2mt$ as an algebraic combination of F_1 and the field equations. Similarly, all polynomials F_i, $i \geq 2$ can be recovered at degree $2mt$ from algebraic combination of F_1 and the field equations. Therefore, the degree of regularity of the original system is smaller than the maximum of $2mt$ and the degree of regularity of the system $\{F_1 = 0; z_{ij}^2 = z_{i,j+1}, i = 1, \ldots, m, j = 1, \ldots, n-1; z_{i,n}^2 = z_{i,1}, i = 1, \ldots, m\}$. Finally like [38], we bound this last degree by the degree of regularity of the subsystem $\{F_1 = 0; z_{ij}^2 = z_{i,j+1}, i = 1, \ldots, m, j = 1, \ldots, t-1\}$.

---

[2] We add a subscript y to the arrows in System (3) to stress that the Weil descent is done on the y_{ij} variables and to distinguish this system from System (2).

Assuming that this system behaves like a generic system with the same degrees and the same number of variables[3], its degree of regularity can be bounded by $m(2t-1)$ using Macaulay's bound. Under this heuristic assumption, we conclude that the degree of regularity of System (3) is bounded by $2mt$.

We point out that the value $2mt$ is already much below the degree of regularity of a generic system of equations (or even a generic *binary* system of equations) with the same degrees [6,7]. Still, our experiments suggest that this bound is not even tight. A tighter bound can be obtained with a seemingly stronger (yet "classical") heuristic assumption.

First fall degree An important characteristic of HFE systems is the existence of many algebraic combinations of the equations that have a degree lower than it would be expected for a generic system. Similar low degree equations were identified for System (2). More precisely, Faugère et al. [33,34] showed that for any monomial $\mathbf{m} \in \mathbb{F}_{2^n}[\mathbf{x_1}, \ldots, \mathbf{x_{n'}}]$, the equations obtained by applying a Weil descent on the polynomial $\mathbf{mf}$ are algebraic combinations of the equations of System (2) that produce a degree fall. By the way they are constructed, the existence of these equations is very specific to polynomial systems arising from a Weil descent. For $\mathbf{m} := \mathbf{x_1}$, we immediately deduce:

Proposition 1. *The first fall degree of System* (2) *is at most* $mt + 1$.

This proposition provides a heuristic explanation for the degrees of regularity observed above since the first fall degree is often a good approximation of the degree of regularity. As recalled in Section 3, this heuristic assumption is "classical" in algebraic cryptanalysis, and it has in particular been verified for various HFE-like systems [38,24,22].

Assumption 1. *Let* $n, m, t, n' \in \mathbb{Z}$. *Let* $\mathbf{f}$ *be generated as in our experiments. For all but a negligible fraction of the resulting systems, we have* $D_{reg} = D_{firstfall} + o(D_{firstfall})$.

The assumption intuitively makes sense for System (2) since not only one but many degree falls are occuring at degree $D_{firstfall}$ and the next ones (each monomial $\mathbf{m}$ leads to new degree falls).

Heuristic complexity bounds for Problem (1) Given the degree of regularity, the complexity of Problem 1 simply follows from the cost of linear algebra.

---

[3] A similar assumption of semi-regularity is needed in [38] to apply Bardet's theorem.

Proposition 2. *If Assumption 1 holds, Problem 1 can be solved with standard Gröbner basis algorithms (like F4 or F5) in time $O(n^{\omega D})$ and memory $O(n^{2D})$, where ω is the linear algebra constant and $D \approx mt$.*

In the univariate case, this estimation reduces to $D \approx t$ which perfectly matches known cryptanalysis results on HFE algebraic systems [30,38]. Interestingly, the special shape of HFE polynomials (they deploy to *quadratic* equations over $\mathbb{F}_2$) seems to have no impact on the degree of regularity (although further restrictions on the shape may have an impact as pointed out in [22]). In the multilinear case, the estimation provided by Proposition 2 becomes $D \approx m$ which matches the experimental data of [33].

As observed in [33,34], the block structure of System (2) can be exploited to accelerate its resolution.

Proposition 3. *If Assumption 1 holds, Problem 1 can be solved with block Gröbner basis algorithms in time $O((n')^{\omega D})$ and memory $O((n')^{2D})$, where ω is the linear algebra constant and $D \approx mt$.*

Additional heuristic methods like hybrid approaches (consisting in mixing exhaustive search and polynomial system resolution [52,9]) may lead to substantial complexity improvements in practice, as was described in [33] for the multilinear case.

5 Index calculus for elliptic curves

We now turn to the main application (so far) of Problem (1). As pointed out in [34], an instance of Problem (1) appears in the relation search step of an index calculus algorithm for elliptic curves proposed by Diem [21]. Given a cyclic (additive) group G, a generator P of this group and another element Q of G, the discrete logarithm problem asks for computing an integer k such that $Q = kP$. Groups typically used in cryptography include the multiplicative groups of finite fields, groups of points on elliptic curves and hyperelliptic curves and Jacobians of higher genus curves. Index calculus algorithms [43,25] with *subexponential* complexities have long been obtained for the multiplicative groups of finite fields [1,16,2,5,39] and more recently for the Jacobian groups of hyperelliptic curves [3,36,35].

In 2004, Semaev introduced his *summation polynomials* and identified their potential application to build index calculus algorithms on elliptic curves [51] over prime fields $\mathbb{F}_p$. These ideas were independently extended by Gaudry [37] and Diem [20] to elliptic curves over composite fields $\mathbb{F}_{p^n}$. Following this approach, Gaudry [37] and later Joux and Vitse [40,41] obtained index calculus algorithms running faster than generic algorithms

for any p and any $n \geq 3$. On the other hand, Diem [20,21] identified some families of curves with a subexponential time index calculus algorithm by letting p and n grow simultaneously in an appropriate way. As far as was known at the moment, the two families of elliptic curves recommended by standards [47] (elliptic curves over prime fields $\mathbb{F}_p$ or over binary fields $\mathbb{F}_{2^n}$ with n prime) remained immune to these attacks. In 2012, Faugère et al. [34] observed that the computation of the relations in an algorithm of Diem for binary fields [21] could be reduced to special instances of Problem (1).

Diem's variant of index calculus Let K be a finite field and let E be an elliptic curve over K defined by the equation $E : y^2 + xy = x^3 + \mathbf{a_2}x^2 + \mathbf{a_6}$ for some $\mathbf{a_2}, \mathbf{a_6} \in \mathbb{F}_{2^n}$. Semaev's *summation polynomials* $\mathbf{S_r}$ are multivariate polynomials satisfying $\mathbf{S_r}(\mathbf{x_1}, \ldots, \mathbf{x_r}) = \mathbf{0}$ for some $\mathbf{x_1}, \ldots, \mathbf{x_r} \in \bar{K}$ if and only if there exist $\mathbf{y_1}, \ldots, \mathbf{y_r} \in \bar{K}$ such that $(\mathbf{x_i}, \mathbf{y_i}) \in E(\bar{K})$ and $(\mathbf{x_1}, \mathbf{y_1}) + \cdots + (\mathbf{x_r}, \mathbf{y_r}) = P_\infty$ [51]. The summation polynomials can be recursively computed as $\mathbf{S_2}(\mathbf{x_1}, \mathbf{x_2}) := \mathbf{x_2} + \mathbf{x_1}$, $\mathbf{S_3}(\mathbf{x_1}, \mathbf{x_2}, \mathbf{x_3}) := \mathbf{x_1}^2\mathbf{x_2}^2 + \mathbf{x_1}^2\mathbf{x_3}^2 + \mathbf{x_1}\mathbf{x_2}\mathbf{x_3} + \mathbf{x_2}^2\mathbf{x_3}^2 + \mathbf{a_6}$ and for any $r \geq 4$, any $k, 1 \leq k \leq r - 3$,
$$\mathbf{S_r}(\mathbf{x_1}, \ldots, \mathbf{x_r}) := \operatorname{Res}_{\mathbf{X}}\left(\mathbf{S_{r-k}}(\mathbf{x_1}, \ldots, \mathbf{x_{m-k-1}}, \mathbf{X}), \mathbf{S_{k+2}}(\mathbf{x_{r-k}}, \ldots, \mathbf{x_r}, \mathbf{X})\right).$$
For $r \geq 2$, the polynomial $\mathbf{S_r}$ is symmetric and has degree 2^{r-2} in every variable $\mathbf{x_i}$ [51].

Summation polynomials were used by Gaudry [37], Joux and Vitse [40] and Diem [20,21] to compute relations in index calculus algorithms for elliptic curves over composite fields. The following variant is an adaptation of Diem [21].

1. **Factor Basis definition.** Fix two integers $m, n' < n$ with $mn' \approx n$ and a vector space $V \subset \mathbb{F}_{2^n}/\mathbb{F}_2$ of dimension n'. Let $\mathcal{F}_V := \{(\mathbf{x}, \mathbf{y}) \in E(K) | \mathbf{x} \in V\}$ be the *factor basis*.
2. **Relation search.** Find about $2^{n'}$ relations $a_i P + b_i Q = \sum_{j=1}^m P_{ij}$ with $P_{ij} \in \mathcal{F}_V$. For each relation,
   (a) Compute $R_i := a_i P + b_i Q$ for random integers a_i, b_i.
   (b) Solve Semaev's polynomial $\mathbf{S_{m+1}}(\mathbf{x_1}, \ldots, \mathbf{x_m}, (R_i)_x)$ with the constraints $\mathbf{x_i} \in V$.
   (c) If there is no solution, go back to (a).
3. **Linear Algebra.** Perform linear algebra on the relations to recover the discrete logarithm value.

In previous works [37,20,21,40], a Weil descent was applied to Semaev's polynomials and the resulting systems were solved with resultants or Gröbner basis algorithms. In these works, the complexity of the relation

search step was derived from the complexity of solving generic systems. However as pointed out in [33,34] and further demonstrated in Section 4 of the present paper, polynomial systems arising from a Weil descent are very far from generic ones.

A new complexity analysis We now revisit Diem's algorithm [21] and its analysis by [34] in accordance with our new analysis of Problem (1). Let n, m, n' be integer numbers. Before starting Diem's algorithm, the $(m+1)$th summation polynomial must be computed. Using Collins' evaluation/interpolation method [15] for the resultant, this can be done in time approximately 2^{t_1} where[4] $t_1 \approx m(m+1)$. We then compute about $2^{n'}$ relations. To obtain these relations, we solve special instances of Problem (1) where $\mathbf{f}(\mathbf{x_1}, \ldots, \mathbf{x_m}) := \mathbf{S_{m+1}}(\mathbf{x_1}, \ldots, \mathbf{x_m}, (a_i P + b_i Q)_x)$ has degree 2^{m-1} with respect to every variable. Since Semaev's polynomials are clearly not random ones, we perform additional experiments.

In our experiments, we apply Diem's algorithm to a randomly chosen binary curve $E : y^2 + xy = x^3 + \mathbf{a_2} x^2 + \mathbf{a_6}$ defined over $\mathbb{F}_{2^n}$, where $n \in \{11, 17\}$. We first fix $m \in \{2, 3\}$ and $n' := \lceil n/m \rceil$. We then generate a random vector space V of dimension n' and a random point R on the curve such that $\mathbf{f}$ has solutions. As in Section 4, we finally use the *Groebner* function of Magma to solve Semaev's equation $\mathbf{S_{m+1}}(\mathbf{x_1}, \ldots, \mathbf{x_m}, R_x) = \mathbf{0}$ with the linear constraints. We repeat this experiment 100 times for each parameter set, then we repeat all our experiments with the Koblitz curve $E : y^2 + xy = x^3 + x^2 + 1$. The average value of the maximal degrees reached during the computation, the average computation time and the maximal memory requirements are reported in Table 2.

Table 2: Average maximal degree reached in Gröbner Basis experiments, average computation time (in seconds) and maximal memory requirements (in MB) for Semaev polynomials. (R): Random curves. (K): Koblitz curves.

E	n	n'	m	t	$mt+1$	D_{av}	Time	Mem.
K	11	6	2	2	5	3.0	0	11
K	11	4	3	3	10	7.1	1	15
K	17	9	2	2	5	4.0	0	15
K	17	6	3	3	10	7.2	132	2133

E	n	n'	m	t	$mt+1$	D_{av}	Time	Mem.
R	11	6	2	2	5	3.0	0	11
R	11	4	3	3	10	7.1	1	15
R	17	9	2	2	5	4.0	0	16
R	17	6	3	3	10	7.1	130	2136

---

[4] To compute $\mathbf{S_{m+1}}$, we apply Collins' algorithm on S_k where $k = \lceil \frac{m+3}{2} \rceil$. This polynomial has degree $2^{\lceil (m-1)/2 \rceil}$ in each variable. Following Collins, Theorem 9, we have $t_1 \le 2(m+1)m/2 = m(m+1)$.

In all cases, the maximal degrees reached in the computations were even *below* the first fall degree bound given by Proposition (1). This phenomenon is probably due to the sparsity of Semaev's polynomials and will be exploited in future work (in particular, the degree of $\mathbf{S_{m+1}}$ with respect to every variable is 2^{m-1} but bounded by $2^m - 1$ in the analysis of Section 4). From now on in the analysis, we ignore this difference and analyze Semaev's polynomials as the random polynomials of Section 4.

Assumption 2. *Assumption 1 still holds if $\mathbf{f}$ is generated from Semaev's polynomials as in the experiments of this section.*

Under Assumption (2), Step 2(b) of Diem's algorithm can be solved using a dedicated Gröbner basis algorithm taking advantage of the block structure, in a time $(n')^{\omega D}$, where $D \approx (m^2+1)$ and ω is the linear algebra constant. Once the x components of a relation have been computed, the y components can be found by solving m quadratic equations and testing each possible combination of the solutions. This requires a time roughly 2^m, that can be neglected. On average, the probability that a point $R_i := a_iP + b_iQ$ can be written as a sum of m points from the factor basis can be heuristically approximated by $\frac{2^{mn'-n}}{m!}$ [21]. Assuming $mn' \approx n$, the total cost of the relation search step can therefore be approximated by 2^{t_2}, where $t_2 \approx m \log m + n' + \omega(m^2 + 1) \log n'$.

The last step of Diem's algorithm consists in (sparse) linear algebra on a matrix of rank about $2^{n'}$ with about m elements of size about n bits per row. This step takes a time approximately equal to $mn2^{\omega'n'} = 2^{t_3}$, where $t_3 \approx \log m + \log n + \omega'n'$ and ω' is the *sparse* linear algebra constant. If Assumption (2) holds and if $mn' \approx n$, the total time taken by Diem's algorithm can be estimated by $T := 2^{t_1} + 2^{t_2} + 2^{t_3}$, where t_1, t_2, t_3 are defined as above.

On the hardness of ECDLP in characteristic 2 We now evaluate the hardness of the elliptic curve discrete logarithm problem over the field $\mathbb{F}_{2^n}$ for "small" values of n. In our estimations, we use $\omega = \log(7)/\log(2)$ and $\omega' = 2$. We consider $n \in \{50, 100, 160, 200, 500, 1000, 2000, 2500, 5000, 10^4, 2 \cdot 10^4, 5 \cdot 10^4, 10^5, 2 \cdot 10^5, 5 \cdot 10^5, 10^6\}$ and $m \in \{2, \ldots, n/2\}$. For every pair of values, we compute values t_1, t_2 and t_3 as above. Finally, we approximate the total running time of Diem's algorithm by $2^{t_{max}}$ where $t_{max} := \max(t_1, t_2, t_3)$. For every value of n, Table 3 presents the data corresponding to the value m for which t_{max} is minimal. We point out that the numbers obtained here have to be taken cautiously since they all rely on Assumption 2 and involve some approximations.

Table 3: Complexity estimates for Diem's algorithm in characteristic 2

n	m	n'	t_1	t_2	t_3	t_{max}	n	m	n'	t_1	t_2	t_3	t_{max}
50	2	25	6	92	57	92	2000	4	500	20	936	1013	1013
100	2	50	6	131	108	131	2500	5	500	30	1166	1014	1166
160	2	80	6	171	168	171	5000	6	833	42	1857	1682	1857
200	2	100	6	195	209	209	10000	7	1429	56	2919	2873	2919
500	3	167	12	379	344	379	20000	9	2222	90	4810	4462	4810
1000	4	250	20	638	512	638	50000	12	4167	156	9105	8353	9105

According to our estimations, Diem's version of index calculus (together with a sparse Gröbner basis algorithm) beats generic algorithms for any $n \geq N$, where N is an integer close to 2000. An actual attack for current cryptographically recommended parameters ($n \approx 160$) seems to be out of reach today, but the numbers in [34] suggest that medium-size parameters could be reachable with additional Gröbner basis heuristics like the hybrid method [9]. Large prime variations [35] of Diem's algorithm may also lead to substantial improvements in practice. This will be investigated in further work.

Letting n grow and fixing $n' := n^\alpha$ and $m := n^{1-\alpha}$ for a positive constant $\alpha < 1$, we obtain

$$t_1 \approx n^{2(1-\alpha)},$$
$$t_2 \approx (1-\alpha)n^{1-\alpha}\log n + n^\alpha + \alpha\omega n^{2(1-\alpha)}\log n,$$
$$t_3 \approx (2-\alpha)\log n + \omega' n^\alpha$$

Taking $\alpha := 2/3$, the relation search dominates the complexity of the index calculus algorithm and we deduce the following result.[5]

Proposition 4. *Under Assumption 2, the discrete logarithm problem over $\mathbb{F}_{2^n}$ can asymptotically be solved in time $O(2^{cn^{2/3}\log n})$, where $c := 2\omega/3$ and ω is the linear algebra constant.*

In particular if the Gaussian elimination algorithm is used for linear algebra, we have $\omega = 3$ and $c = 2$. We stress that Proposition 4 holds even when n is prime. Until now, the best complexity estimates obtained in that case corresponded to generic algorithms that run in time $2^{n/2}$.

---

[5] Note that the weaker bound $D_{reg} \leq 2mt$ derived in Section 4 with Macaulay's bound also leads to a subexponential complexity but with a constant $c = 4\omega/3$.

6 Conclusion and perspectives

In this paper, we revisited the complexity of solving polynomial systems arising from a Weil descent, a class of polynomial systems previously introduced by Faugère et al. [33,34]. We observed that these systems can be seen as natural extensions of HFE systems and we generalized various results on HFE. Based on experimental results and heuristic arguments, we conjectured that the degree of regularity of these systems are only slightly larger than their original degrees, and we deduced new heuristic bounds on their resolution. Interestingly, our bounds nicely generalize previous bounds on HFE.

The most proeminent consequence of our analysis so far concerns the elliptic curve discrete logarithm problem (ECDLP) over binary fields. Indeed, our heuristic analysis suggests that ECDLP can be solved in *subexponential* time $O(2^{c\,n^{2/3}\log n})$ over the binary field $\mathbb{F}_{2^n}$, where c is a constant smaller than 2. This complexity is obtained with an index calculus algorithm due to Diem [20] and a block-structured Gröbner basis algorithm. In practice, our estimations predict that the resulting algorithm is faster than generic algorithms (previously thought to be the best algorithms for this problem) for any n larger than N, where N is an integer approximately equal to 2000. In particular, binary elliptic curves of currently recommended sizes ($n \approx 160$) are not immediately threatened.

Our complexity estimates are based on heuristic assumptions that differ from other index calculus algorithms, but are common in algebraic cryptanalysis. The polynomial systems appearing in the cryptanalysis of HFE have been intensively studied in the last 15 years, yet we have no definitive proof for their commonly admitted complexity. Our paper broadens the interest of these researches to all polynomial systems arising from a Weil descent and to their various applications. We leave further experimental and theoretical investigation of our heuristic assumptions to further work.

To conclude this paper, we point out that most of our results generalize quite easily to other fields, resulting in comparable asymptotic complexities.

References

1. Leonard M. Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography (abstract). In *FOCS*, pages 55–60. IEEE, 1979.
2. Leonard M. Adleman. The function field sieve. In Adleman and Huang [4], pages 108–121.
3. Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh A. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In Adleman and Huang [4], pages 28–40.
4. Leonard M. Adleman and Ming-Deh A. Huang, editors. *Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, May 6-9, 1994, Proceedings*, volume 877 of *Lecture Notes in Computer Science*. Springer, 1994.
5. Leonard M. Adleman and Ming-Deh A. Huang. Function field sieve method for discrete logarithms over finite fields. *Inf. Comput.*, 151(1-2):5–16, 1999.
6. Magali Bardet. *Etude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, Université Paris 6, 2004.
7. Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *International Conference on Polynomial System Solving - ICPSS*, pages 71 –75, Nov 2004.
8. Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. In P. Gianni, editor, *The Effective Methods in Algebraic Geometry Conference, Mega 2005*, pages 1 –14, May 2005.
9. Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2010.
10. Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of multivariate and odd-characteristic hfe variants. In Catalano et al. [14], pages 441–458.
11. Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic. *Des. Codes Cryptography*, pages 1–42, 2012. accepted.
12. Charles Bouillaguet, Jean-Charles Faugère, Pierre-Alain Fouque, and Ludovic Perret. Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In Catalano et al. [14], pages 473–493.
13. Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Universitt Innsbruck, 1965.
14. Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors. *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*. Springer, 2011.
15. George Collins. The calculation of multivariate polynomial resultants. *Journal of the Association for Computing Machinery*, 18:515–522, 1971.
16. Don Coppersmith. Fast evaluation of logarithms in fields of characteristic two. *IEEE Transactions on Information Theory*, 30(4):587–593, 1984.
17. Nicolas Courtois. The security of hidden field equations (HFE). In David Naccache, editor, *CT-RSA*, volume 2020 of *Lecture Notes in Computer Science*, pages 266–281. Springer, 2001.

18. Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *EUROCRYPT*, pages 392–407, 2000.

19. David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer Verlag, Berlin, Heidelberg, New York, 1 edition, 1992.

20. Claus Diem. On the discrete logarithm problem in elliptic curves. *Compositio Mathematica*, 147:75–104, 2011.

21. Claus Diem. On the discrete logarithm problem in elliptic curves II. 2011. `http://www.math.uni-leipzig.de/~diem/preprints/dlp-ell-curves-II.pdf`.

22. Jintai Ding and Timothy J. Hodges. Inverting HFE systems is quasi-polynomial for all fields. In *CRYPTO*, pages 724–742, 2011.

23. Jintai Ding and Thorsten Kleinjung. Degree of regularity for HFE-. *IACR Cryptology ePrint Archive*, 2011:570, 2011.

24. Vivien Dubois and Nicolas Gama. The degree of regularity of HFE systems. In *ASIACRYPT*, pages 557–576, 2010.

25. Andreas Enge and Pierrick Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arith.*, 102(1):83–103, 2002.

26. Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.

27. Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

28. Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In *ISSAC*, pages 257–264, 2010.

29. Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity. *J. Symb. Comput.*, 46(4):406–437, 2011.

30. Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2003.

31. Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. Algebraic cryptanalysis of mceliece variants with compact keys. In Henri Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 279–298. Springer, 2010.

32. Jean-Charles Faugère and Ludovic Perret. Polynomial equivalence problems: Algorithmic and theoretical aspects. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 30–47. Springer, 2006.

33. Jean-Charles Faugère, Ludovic Perret, Christophe Petit, and Guénaël Renault. New subexponential algorithms for factoring in $SL(2, \mathbb{F}_{2^n})$. Cryptology ePrint Archive, Report 2011/598, 2011. `http://eprint.iacr.org/`.

34. Jean-Charles Faugère, Ludovic Perret, Christophe Petit, and Guénaël Renault. Improving the complexity of index calculus algorithms in elliptic curves over binary fields. In Pointcheval and Johansson [50], pages 27–44.

35. P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp.*, 76(257):475–492 (electronic), 2007.

36. Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *Lecture Notes in Computer Science*, pages 19–34. Springer, Berlin, 2000.

37. Pierrick Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *J. Symb. Comput.*, 44(12):1690–1702, 2009.

38. Louis Granboulan, Antoine Joux, and Jacques Stern. Inverting HFE is quasipolynomial. In Cynthia Dwork, editor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 345–356. Springer, 2006.

39. Antoine Joux and Reynald Lercier. The function field sieve in the medium prime case. In *Advances in cryptology—EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Comput. Sci.*, pages 254–270. Springer, Berlin, 2006.

40. Antoine Joux and Vanessa Vitse. Elliptic Curve Discrete Logarithm Problem over Small Degree Extension Fields. Application to the static Diffie-Hellman problem on $E(\mathbb{F}_{q^5})$. Cryptology ePrint Archive, Report 2010/157. To appear in Journal of Cryptology., 2010. `http://eprint.iacr.org/`.

41. Antoine Joux and Vanessa Vitse. Cover and decomposition index calculus on elliptic curves made practical - application to a previously unreachable curve over $\mathbb{F}_{p^6}$. In Pointcheval and Johansson [50], pages 9–26.

42. Aviad Kipnis and Adi Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In Michael J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

43. Maurice Kraitchik. *Théorie des nombres*. Gauthier-Villars, 1922.

44. Daniel Lazard. Gröbner-bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proceedings of the European Computer Algebra Conference on Computer Algebra*, volume 162 of *Lecture Notes in Computer Science*, Berlin, Heidelberg, New York, 1983. Springer Verlag.

45. F.S. Macaulay. *The algebraic theory of modular systems.*, volume XXXI of *Cambridge Mathematical Library*. Cambridge University Press, 1916.

46. F.S. Macaulay. Some properties of enumeration in the theory of modular systems. *Proc. London Math. Soc.*, 26:531–55, 1927.

47. National Institute of Standards and Technology. Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-3, 2009.

48. Jacques Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In Ueli M. Maurer, editor, *EUROCRYPT*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

49. Christophe Petit and Jean-Jacques Quisquater. On polynomial systems arising from a weil descent. Cryptology ePrint Archive, Report 2012/146, 2012. `http://eprint.iacr.org/`.

50. David Pointcheval and Thomas Johansson, editors. *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*. Springer, 2012.

51. Igor Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Available at `http://www.isg.rhul.ac.uk/~ppai034/_pub/papers/Semaev%20%28Feb%29.pdf`, 2004.

52. Bo-Yin Yang, Jiun-Ming Chen, and Nicolas Courtois. On asymptotic security estimates in XL and Gröbner bases-related algebraic cryptanalysis. In Javier Lopez, Sihan Qing, and Eiji Okamoto, editors, *ICICS*, volume 3269 of *Lecture Notes in Computer Science*, pages 401–413. Springer, 2004.