Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach

Luk Bettale, Jean-Charles Faugère, Ludovic Perret

Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach

Luk Bettale*
Oberthur Technologies
71-73 rue des Hautes Pâtures
92726 Nanterre Cedex,
France
l.bettale@oberthur.com

Jean-Charles Faugère
INRIA
Paris-Rocquencourt Center
PolSys Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6
Case 169, 4, Place Jussieu,
F-75252 Paris
Jean-Charles.Faugere@inria.fr

Ludovic Perret
INRIA
Paris-Rocquencourt Center
PolSys Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6
Case 169, 4, Place Jussieu,
F-75252 Paris
Ludovic.Perret@lip6.fr

ABSTRACT

The Polynomial System Solving (PoSSo) problem is a fundamental NP-Hard problem in computer algebra. Among others, PoSSo have applications in area such as coding theory and cryptology. Typically, the security of multivariate public-key schemes (MPKC) such as the UOV cryptosystem of Kipnis, Shamir and Patarin is directly related to the hardness of PoSSo over finite fields. The goal of this paper is to further understand the influence of finite fields on the hardness of PoSSo. To this end, we consider the so-called *hybrid approach*. This is a polynomial system solving method dedicated to finite fields proposed by Bettale, Faugère and Perret (Journal of Mathematical Cryptography, 2009). The idea is to combine exhaustive search with Gröbner bases. The efficiency of the hybrid approach is related to the choice of a trade-off between the two methods. We propose here an improved complexity analysis dedicated to quadratic systems. Whilst the principle of the hybrid approach is simple, its careful analysis leads to rather surprising and somehow unexpected results. We prove that the optimal trade-off (i.e. number of variables to be fixed) allowing to minimize the complexity is achieved by fixing a number of variables proportional to the number of variables of the system considered, denoted n. Under some natural algebraic assumption, we show that the asymptotic complexity of the hybrid approach is $2^{(3.31-3.62\log_2(q)^{-1})n}$, where q is the size of the field (under the condition in particular that $\log(q) \ll n$). This is to date, the best complexity for solving PoSSo over finite fields (when $q > 2$). We have been able to quantify the gain provided by the hybrid approach compared to a direct Gröbner basis method. For quadratic systems, we show (assuming a natural algebraic assumption) that this gain is exponential in the number of variables. Asymptotically, the gain is $2^{1.49n}$ when both n and q grow to infinity and $\log(q) \ll n$.

*This work has been carried out when this author was PhD student at UPMC/INRIA/LIP6).

1. INTRODUCTION

The purpose of this paper is to study the complexity of solving the Polynomial System Solving (PoSSo) problem over finite fields. This problem, that will be denoted by PoSSo_q, is as follows:

Polynomial System Solving over Finite Fields (PoSSo_q)
Let $q = p^k$, where p is prime and $k > 0$.
Input: $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n) \in \mathbb{F}_q[x_1,\ldots,x_n]$.
Goal: find a vector $z_1,\ldots,z_n \in \mathbb{F}_q^n$ such that:

$$f_1(z_1,\ldots,z_n) = \cdots = f_m(z_1,\ldots,z_n) = 0.$$

PoSSo_q typically arises in area such as cryptography and coding theory (but not limited to). In cryptology, the hardness of PoSSo_q is now a subject of major interest, e.g. [30, 23, 24, 16, 18, 14, 17, 25, 1, 29, 15, 34, 36, 21]. In one hand, this problem is used as a trapdoor to design many cryptographic primitives, mostly in multivariate cryptography [32, 33, 37]. On the other hand, the security of many cryptosystems reduce trough algebraic attacks [3, 23, 35] to PoSSo_q.

From a complexity-theoretical point of view, PoSSo_q is NP-Hard independently of the size q [28]. Thus, any algorithm for PoSSo_q should be exponential in the worth case. However, this does not exclude that large family of PoSSo_q instances can be solved in sub-exponential or polynomial complexity. In addition, the exact exponent occurring in algorithms of exponential complexity is often a critical question in applications.

The general question we want to address here is how much the restriction to finite fields influence the hardness of PoSSo ?

Hybrid Approach. In [9], we have described a rather simple Gröbner-basis based method taking advantage of the finite field structure: the so-called *hybrid approach*. The idea is to mix exhaustive search and Gröbner bases [11, 13, 12] computation. In what follows, hybrid approach will always refer to the Gröbner-basis based method described in [9]. The principle of such approach is to fix k – which is a parameter – among the n variables of the system considered and then compute q^k Gröbner bases of smaller systems to recover the set of solutions. The efficiency of the hybrid approach depends upon a proper choice of the *trade-off* k between the number of variables to be fixed and the cost of computing a Gröbner basis of the smaller sub-systems. At first glance, it is even not clear that a non-trivial trade-off exists (i.e.

whether $k \neq 0$?). A first contribution of [9] is to show that the hybrid approach brings a significant improvement in practice (with respect to a direct Gröbner basis computation). As an application, we have shown that the parameters of many multivariate schemes (which are directly based on the hardness of PoSSo_q) must be refined to achieve a cryptographic security level (i.e. $> 2^{80}$ operations). For instance, the hybrid approach has been used to attack previously recommended parameters of the UOV scheme [29] (for instance, [9][Table 4, first row] in a complexity as small as $2^{37.75}$). Remark that experiments performed in [9] suggest that the optimal trade-off seems to be achieved for a small and constant value of k. We show in this paper that this intuition is actually false.

We mention that [9] also laid the foundation for a theoretical analysis of the hybrid approach. It has been shown that the hybrid approach is beneficial (i.e. a non-trivial trade-off exists) if q is less than $2^{0.62\,\omega n}$, where $\omega, 2 \leqslant \omega \leqslant 3$ is the linear algebra constant.

Related Works. The complexity of solving solving binary quadratic equations has been more particularly investigated in [38, 39, 7]. The authors of [38] proposed an heuristic method – based on the so-called XL [31] algorithm – of complexity $O\left(2^{0.875n}\right)$ for solving PoSSo_2 (with quadratic equations). They propose to combine exhaustive search with XL. This is the so-called FXL. As pointed in [2] XL can be viewed as a sub-optimal version of F_4 [19] (and consequently, FXL is a sub-optimal version of the hybrid approach). In addition, the exact assumptions that have to be verified by the input systems are unclear. Also, similar results have been announced in [39][Section 2.2], but there analysis relies on algorithmic assumptions (e.g., row echelon form of sparse matrices in quadratic complexity) that are not known to hold currently. Under these assumptions, the authors show that the most favorable trade-off between exhaustive search and row echelon form computations in the FXL algorithm is obtained by specializing $0.45n$ variables (for $q = 2$). Recently, [7] used an hybrid approach – and additional techniques – to further improve the solving of quadratic binary systems. The authors of [7] proposed a deterministic algorithm for solving PoSSo_2 in $O\left(2^{0.841n}\right)$ when $m = n$ (i.e. same number of equations and variables). A probabilistic variant of their algorithm (Las Vegas type) has expected complexity $O\left(2^{0.792n}\right)$. They roughly estimate the actual threshold between their method and exhaustive search (whose cost is $4\log_2 n 2^n$ operations [10]), which is as low as 200. Note that the complexity analysis in [7] requires an algebraic assumption which is similar to [9]. Such assumption will be also used here. From now on, we will always assume that $q > 2$.

The question of solving PoSSo_q for a bigger q is quickly addressed in [39][Section 2.1]. More precisely, [39][Proposition 7, p. 5] describes an implicit method for finding the optimal number of variables to be fixed in FXL. For $q = 2^8$, the best-tradeoff in FXL is obtained by fixing $0.049n$ variables (assuming $\omega = 2$). Using a different technique, we present also here an implicit method for finding the best-tradeoff with the hybrid approach. For example with $q = 2^8$, we get the most favorable trade-off is obtained by fixing $0.07n$ variables (assuming $\omega = 2.4$).

The goal of this paper is to further improve the theoretical analysis initiated in [9]. In particular, we address the following issues:

- What is the explicit asymptotic value of the best trade-off ?
- What is the asymptotic complexity the hybrid approach ?
- What is the gain of the hybrid approach over a direct Gröbner basis method ?

Organization of the Paper. After this introduction, the paper is organized as follows. Sect. 2 recalls some results from [9] needed for our new analysis. We also define a general framework for our study. We emphasize that all our results are based on a rather natural algebraic assumption about the sub-systems considered during the hybrid approach, i.e. we assume that semi-regular system remains semi-regular after having specialized some variables (this is similar to [9, 7]). This is formalized in Hypothesis 1 (Section 2.1). In Section 2.2, we present a first new result about the hybrid approach. Surprisingly enough, we have been able to show that fixing a number of variables k which is proportional to the initial number of variables of the system considered yields a better trade-off than the one in [9]. In Section 3, we provide an explicit form of the best trade-off. We show that it is asymptotically[1] equivalent to:

$$n\,\frac{10.86\,\omega^2}{\left(4.16\log_2(q) - 3.14\,\omega\right)^2},$$

where $\omega, 2 \leqslant \omega \leqslant 3$ is the linear algebra constant.

This result allows to derive an asymptotical equivalent for the cost of the hybrid approach. Precisely, the complexity is asymptotically equivalent to

$$2^{n\omega\left(1.38 - 0.44\,\omega\log(q)^{-1}\right)},\ \text{when } n \to \infty, q \to \infty \text{ and } \log(q) \ll n.$$

Finally, we quantify in Section 4 the gain of the hybrid approach with respect to a direct Gröbner basis computation. Once again, we arrive to a rather unexpected result. The hybrid approach provides – under some conditions – an exponential speed-up. More precisely, when $n \to \infty, q \to \infty$ and as long as $n \gg \log(q)$, the gain of the hybrid approach compared to the direct Gröbner basis approach is asymptotically $2^{0.62\,\omega n}$. To the knowledge of the authors, this makes the hybrid approach the method with the best asymptotical complexity for solving PoSSo_q (for $q > 2$).

2. PRELIMINARIES

We review in this part some useful results obtained in [9]. Throughout the paper, we always use the following notations: q is the size of the field, n is the number of variables, m is the number of equations and k is the *trade-off* (number of fixed variables in the hybrid approach). We will always assume that $m \geq n$. We denote by $\omega, 2 \leqslant \omega \leqslant 3$ the linear algebra constant. We write O for the "big O" notation. We also use the o for the "little-o" notation, i.e. $f(n) = o\big(g(n)\big)$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$. Finally, we say that f and g are asymptotically equivalent, denoted $f \sim g$, if $f - g = o(g)$ (or equivalently, $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$ if f and g are positive real valued functions).

2.1 Complexity of the Hybrid Approach

We recall in this part the general expression of the hybrid approach cost [9]. To do so, let $C_{\mathrm{F}_5}\left(n, m, d_{\mathrm{reg}}\right)$ be the complexity of computing the Gröbner basis of a system of m equations in n variables using the F_5 algorithm[2] [20], where d_{reg} is the *degree of regularity* of the system. Informally, the degree of regularity is the maximum degree reached during the Gröbner basis computation. Note that this degree depends on n, m and q. The complexity of the hybrid approach [9] is as follows.

PROPOSITION 2.1. *Let $\{f_1, \ldots, f_m\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be an algebraic system of equations with respective degrees $d_1 \geqslant \cdots \geqslant d_m$.*

[1] A maple code corresponding to this paper can be found at `http://www-salsa.lip6.fr/~perret/Site/hybrid_issac.mpl`.

[2] Note that a similar analysis could be also performed with any algorithm solving PoSSo_q and having a precise complexity estimates based on the degree of regularity, e.g. [11, 13, 12, 19, 20, 27].

Let k be a non-negative integer and $\mathrm{d}_{reg}^{max}(k)$ (resp. $\mathrm{D}^{max}(k)$) be the maximum degree of regularity (resp. maximum number of solutions in the algebraic closure of $\mathbb{F}_q$ counted with multiplicities) of all the systems:

$$\{f_1(x_1,\ldots,x_{n-k},v_1,\ldots,v_k),\ldots,f_m(x_1,\ldots,x_{n-k},v_1,\ldots,v_k)\}$$

for any $(v_1,\ldots,v_k)\in\mathbb{F}_q^k$. The complexity of the hybrid approach is bounded from above by:

$$\min_{0\leqslant k\leqslant n}\left(q^k\left(\underbrace{C_{F_5}\left(n-k,m,\mathrm{d}_{reg}^{max}(k)\right)}_{\text{Gröbner basis}}+\underbrace{O\left((n-k)\,\mathrm{D}^{max}(k)^{\omega}\right)}_{\text{change of ordering}}\right)\right). \quad (1)$$

This is the complexity of computing q^k (DRL) Gröbner bases with F_5 of polynomial systems having m equations, $n-k$ variables, respective degrees $d_1\geqslant\cdots\geqslant d_m$, plus the cost of performing a change of ordering with FGLM [22].

In order to study the asymptotical behavior of the hybrid approach, we assume – as in [9] – a regularity condition about the sub-systems arising during the hybrid approach.

HYPOTHESIS 1. *Let $\{f_1,\ldots,f_m\}\subset\mathbb{F}_q[x_1,\ldots,x_n]$ be random algebraic equations of respective degrees $d_1\geqslant\cdots\geqslant d_m$.*
Let $\beta_{\min}, 0<\beta_{\min}<1$ be a value that will be specified later. Then, for any $k, 0\leqslant k\leqslant\lceil\beta_{\min}n\rceil$, and for each vector $(v_1,\ldots,v_k)\in\mathbb{F}_q^k$, the system:

$$\{f_1(x_1,\ldots,x_{n-k},v_1,\ldots,v_k),\ldots,f_m(x_1,\ldots,x_{n-k},v_1,\ldots,v_k)\}$$

is semi-regular for n large enough.

Note that systems verifying such hypothesis are in particular semi-regular ($k=0$). We refer the reader to [8, 4, 6, 5] for more information on semi-regular systems. In practice, a randomly picked system is semi-regular with high probability. Assuming Fröberg's conjecture [26], this can be proven more formally. We emphasize that Hypothesis 1 has been experimentally verified [7] for a large amount of random quadratic binary systems. In [9], such assumption has been verified for larger q on algebraic systems coming coming from multivariate schemes such as UOV [30]. However, such systems are naturally under-defined. Thus, the total number of variables to be fixed ($m-n$ variables to have a square system plus k variables due to the hybrid approach) is sufficiently big to assume that the algebraic systems obtained after specialization behave as a random system. Note also that we performed some experiments to check this assumption for random systems of equations. We experimentally verified that Hypothesis 1 holds for random square systems with various values of $n, 6\leq n\leq 16$, and with parameters $q,\beta_{\min}$ as in Table 2.

One interesting feature of semi-regular systems is that their degree of regularity is known in advance. Indeed, let $\{f_1,\ldots,f_m\}\subset\mathbb{F}_q[x_1,\ldots,x_n]$ be a semi-regular system. Its regularity is given by the index of the first non-positive coefficient of

$$\sum_{k\geq 0}c_k z^k=\frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}.$$

In addition, asymptotical equivalents are known [8, 4, 6, 5] for the degree of regularity. These allow to perform the analysis in [9], and will be further used in this paper.

Note that assuming Hypothesis 1, all the sub-systems solved during the hybrid approach have – for a fixed k – the same degree of regularity. We denote this regularity by $\mathrm{d}_{\mathrm{reg}}(k)$ (i.e. $\mathrm{d}_{\mathrm{reg}}^{\max}(k)=\mathrm{d}_{\mathrm{reg}}(k)$. Furthermore, the number of solutions of an over-determined semi-regular system of equations is always 0 or 1 (i.e. $0\leq\mathrm{D}^{\max}(k)\leq 1$ as soon as $k>0$). This allows to neglect the cost of the change ordering algorithm in the complexity.

2.2 Best Trade-Off for Quadratic Systems ?

Throughout this paper, we denote by k_0 the optimal value for k, that is, the parameter that minimizes the complexity of the hybrid approach. The goal of this part is to have the asymptotic trend of the best trade-off. To simplify the analysis, we focus our attention to quadratic systems. Such systems are widespread in many applications (especially cryptography), making their study of main interest.

To find the best trade-off, we want to minimize the complexity of the hybrid approach. To do so, we first consider the complexity $C_{\mathrm{hyb}}(k)$ of the hybrid approach as a continuous function of $k\in\mathbb{R}$. When this function reaches its minimum, its derivative $C_{\mathrm{hyb}}(k)'$ with respect to k vanishes. A root k_0 of $C_{\mathrm{hyb}}(k)'$ with $k_0, 0\leqslant k_0\leqslant n$ gives then the best tradeoff. Finally, as $C_{\mathrm{hyb}}(k)$ is a complexity, it is always positive. It is thus equivalent to look for a root of its logarithmic derivative $\frac{C_{\mathrm{hyb}}(k)'}{C_{\mathrm{hyb}}(k)}$.

Let $C_1(n,k)=(n-k-1)\,,C_2(n,k)=\left(\frac{3n-k}{2}-1-\sqrt{nk}\right)$ and $C_3(n,k)=\left(\frac{n+k}{2}-\sqrt{nk}\right)$. The authors of [9] obtain that the best trade-off k_0 is a root of $\Delta(k)$ where

$$\begin{aligned}\Delta(k)=\log(q)+\omega\left(\log\left(C_1(n,k)\right)+\frac{1}{2C_1(n,k)}\right)\\ -\frac{\omega}{2}\left(1+\sqrt{n/k}\right)\left(\log\left(C_2(n,k)\right)+\frac{1}{2C_2(n,k)}\right)\\ -\frac{\omega}{2}\left(1-\sqrt{n/k}\right)\left(\log\left(C_3(n,k)\right)+\frac{1}{2C_3(n,k)}\right).\end{aligned} \quad (2)$$

To push further the asymptotical analysis, we need to assume – a priori – what it is the global trend of k. At first glance, it seems (rather) natural to believe that k is going to be small and should be then a constant. This is what was assumed in [9]. Surprisingly enough, we will see that the best trade-off is obtained asymptotically by fixing $\beta_0 n$ variables, where β_0 is independent of n.

To do this, we first write $k=\beta n$ with $0\leqslant\beta\leqslant 1$, and we show that β tends to a constant when n grows to infinity. By substituting k by βn in (2), and factoring by n in each log terms we obtain that $\Delta(\beta)=$

$$\begin{aligned}&\log(q)+\omega\left(\log(n)+\log\left(1-\beta-\frac{1}{n}\right)+\frac{1}{2C_1(n,\beta n)}\right)\\ &-\frac{\omega}{2}\left(1+\sqrt{1/\beta}\right)\left(\log(n)+\log\left(\frac{3-\beta}{2}-\frac{1}{n}-\sqrt{\beta}\right)+\frac{1}{2C_2(n,\beta n)}\right)\\ &-\frac{\omega}{2}\left(1-\sqrt{1/\beta}\right)\left(\log(n)+\log\left(\frac{1+\beta}{2}-\sqrt{\beta}\right)+\frac{1}{2C_3(n,\beta n)}\right).\end{aligned} \quad (3)$$

The coefficient of $\log(n)$ in this expression is:

$$\left(\omega-\frac{\omega}{2}\left(1+\sqrt{1/\beta}\right)-\frac{\omega}{2}\left(1-\sqrt{1/\beta}\right)\right)=0.$$

We remark that $C_1(n,\beta n), C_2(n,\beta n)$ and $C_3(n,\beta n)$ go to infinity when n tends to infinity. As a consequence:

$$\begin{aligned}\Delta(\beta)\sim\log(q)+\omega\left(\log(1-\beta)\right)\\ -\frac{\omega}{2}\left(1+\sqrt{1/\beta}\right)\left(\log\left(\frac{3-\beta}{2}-\sqrt{\beta}\right)\right)\\ -\frac{\omega}{2}\left(1-\sqrt{1/\beta}\right)\left(\log\left(\frac{1+\beta}{2}-\sqrt{\beta}\right)\right).\end{aligned}$$

Observe that n does not appear in the asymptotic expansion of $\Delta(\beta)$. Thus, a solution of $\Delta(\beta)=0$ at infinity is unrelated to n. As a consequence, the best (asymptotic) trade-off can be written

$k_0 = \beta_0 n$, where β_0 is unrelated to n. This is a contradiction with our prior assumption [9]: k_0 is not a constant. To have a precise analysis, we should look for the best asymptotic trade-off assuming $k = \beta n$. This is one of the reasons motivating a new analysis.

3. COMPLEXITY OF HYBRID APPROACH

In this part, we investigate the complexity of the hybrid approach. The goal is to have an expression of the complexity as explicit as possible. To this end, we first derive an asymptotical equivalent of this complexity depending of the degree of regularity. According to Section 2.2, we have the global trend of the best trade-off. It is of the form $k = \beta n$ (with β unrelated to n). Then, we derive an asymptotically equivalent formula for the regularity of the sub-systems involved in the hybrid approach. Finally, we put everything together to get an asymptotic equivalent for hybrid approach cost.

3.1 A First Asymptotic Equivalent

We recall that the complexity of F_5 as stated in [8]:

$$C_{F_5}\left(n, d_{\text{reg}}\right) = O\left(\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right). \tag{4}$$

Remark that this complexity does not involve explicitly the number of equations (m). But, remember the regularity depends on m. This cost is slightly different from the one used in [9]. The reason is that (4) is more accurate for semi-regular systems.

Using Stirling's formula, i.e.

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n,$$

we can derive a first expression for complexity of the hybrid approach. Since $C_{\text{hyb}}(k) = q^k C_{F_5}\left(n-k, \text{dreg}(k)\right)$, it is not difficult to see that $C_{\text{hyb}}(k) \sim$

$$q^k\left(\frac{1}{\sqrt{2\pi}} \cdot \frac{\left(n-k+\text{dreg}(k)\right)^{n-k+\text{dreg}(k)+\frac{1}{2}}}{\left(n-k\right)^{n-k+\frac{1}{2}}\ \text{dreg}(k)^{\text{dreg}(k)+\frac{1}{2}}}\right)^{\omega}. \tag{5}$$

By abuse of language, we will always refer to (5) (asymptotic equivalent) as the complexity of the hybrid approach.

3.2 Asymptotic Equivalent of the Regularity

From now on, we set $m = \alpha n$ ($\alpha \geq 1$ is a constant). According to Section 2.2, the best trade-off is obtained for a k of the form $\beta \cdot n$. Thus, the hybrid approach considers sub-systems having $n' = n(1-\beta)$ variables and a number of equations $m = \frac{\alpha}{1-\beta}(1-\beta)n = \theta n'$. For such systems, we have an asymptotic equivalent of the degree of regularity [8], i.e.:

$$d_{\text{reg}}(n', m) \sim \left(\theta - \frac{1}{2} - \sqrt{\theta(\theta-1)}\right)n + O\left(n^{1/3}\right). \tag{6}$$

Note that in [9], we have used a different asymptotic expansion of the degree of regularity. Experiments performed in [9] seem to suggest that the optimal number of variables (i.e. trade-off) to be fixed is a constant. As discussed in Section 2.2, this intuition is incorrect.

Thus, assuming a trade-off of the form $\beta \cdot n$, we get that any sub-system occurring in the hybrid approach has a degree of regularity asymptotically equivalent to $\gamma n + O\left(n^{1/3}\right)$, with:

$$\gamma = \left(\alpha - \frac{1-\beta}{2} - \sqrt{\alpha\left(\alpha+\beta-1\right)}\right). \tag{7}$$

3.3 Implicit Form of the Best Trade-Off

In this part, we show that the best trade-off at infinity $k_0 = \lceil \beta_0 n \rceil$ can be obtained by solving an implicit equation. The idea is to derive an equivalent of the logarithmic derivative of C_{hyb} using the regularity (7). Let $D = 1 - \beta + \gamma$. By combining (2) and (7), we get that $\frac{C_{\text{hyb}}(\beta n)'}{C_{\text{hyb}}(\beta n)} \sim$

$$\begin{aligned} n\log(q) + \omega n\left(\log(n) + \log(1-\beta) + \frac{1}{2n(1-\beta)}\right) \\ - \frac{\omega n}{2}\left(1+\sqrt{\frac{\alpha}{\alpha+\beta-1}}\right)\left(\log(n)+\log(D)+\frac{1}{2nD}\right) \\ - \frac{\omega n}{2}\left(1-\sqrt{\frac{\alpha}{\alpha+\beta-1}}\right)\left(\log(n)+\log(\gamma)+\frac{1}{2n\gamma}\right). \end{aligned}$$

The terms in $\log(n)$ cancel out in this expression. Since $n > 0, \beta_0$ is then a root of $A(\beta) = \frac{1}{n} \cdot \frac{C_{\text{hyb}}(\beta n)'}{C_{\text{hyb}}(\beta n)}$. By ignoring constant terms at infinity:

$$A(\beta) \sim A_\infty(\beta), \tag{8}$$

with

$$\begin{aligned} A_\infty(\beta) \quad = \quad & \log(q) + \omega\log(1-\beta) \\ & -\frac{\omega}{2}\left(1+\sqrt{\frac{\alpha}{\alpha+\beta-1}}\right)\log\left(D_1(\alpha,\beta)\right) \\ & -\frac{\omega}{2}\left(1-\sqrt{\frac{\alpha}{\alpha+\beta-1}}\right)\log\left(D_2(\alpha,\beta)\right), \end{aligned}$$

where $D_1(\alpha,\beta) = \alpha + \frac{1-\beta}{2} - \sqrt{\alpha\left(\alpha+\beta-1\right)}$ and $D_2(\alpha,\beta) = \alpha - \frac{1-\beta}{2} - \sqrt{\alpha\left(\alpha+\beta-1\right)}$. This leads to the following result.

PROPOSITION 3.1. *Let $\mathscr{F} = \{f_1, \ldots, f_m\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a system of quadratic equations verifying Hypothesis 1. Let A_∞ be as defined in* (8)*. The best trade-off for solving $\mathscr{F}$ with the hybrid approach is asymptotically to fix $k_0 = \lceil \beta_0 n \rceil$ variables, where β_0 is a root of A_∞ such that $\beta_0, 0 < \beta_0 \leqslant 1$. The coefficient β_0 is independent on the number of variables n.*

A root β_0 of $A_\infty(\beta)$ can be computed numerically (for instance using a computer algebra software like MAPLE). In Table 2 (Appendix), we present the best trade-off β_0 obtained for various values of α and q.

3.3.1 *Square Quadratic Systems*

In this part, we focus on the common case $m = n$ (i.e., $\alpha = 1$, square system). This allows to further refine Proposition 3.1. First, we simplify $A_\infty(\beta)$ as defined in (8) by setting $\alpha = 1$. Second, we make the change of variable $\beta \leftarrow \frac{1}{\nu^2}$. Finally, by expending $B_\infty(\nu) = A_\infty\left(\frac{1}{\nu^2}\right)$, we get that:

$$\begin{aligned} B_\infty(\nu) = \log(q) + \omega\log(2\nu+2) + \omega\log\left(\frac{\nu-1}{2\nu^2}\right) \\ - \frac{\omega}{2}(1+\nu)\log(3\nu+1) - \frac{\omega}{2}(1+\nu)\log\left(\frac{\nu-1}{2\nu^2}\right) \\ - \frac{\omega}{2}(1-\nu)\log(\nu-1) - \frac{\omega}{2}(1-\nu)\log\left(\frac{\nu-1}{2\nu^2}\right). \end{aligned}$$

We observe that the terms in $\log\left(\frac{\nu-1}{2\nu^2}\right)$ cancels out. Finally:

$$A(\beta) \sim B_\infty(\beta), \tag{9}$$

with $B_\infty(\nu) = \log(q) +$

$$\omega\left(\log(2\nu+2) - \frac{1+\nu}{2}\log(3\nu+1) - \frac{1-\nu}{2}\log(\nu-1)\right).$$

For square systems, Proposition 3.1 can be refined as follows.

PROPOSITION 3.2. *Let $\mathscr{F} = \{f_1, \ldots, f_n\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a system of quadratic equations verifying Hypothesis 1. Let B_∞ be as defined in* (9). *The best trade-off for solving $\mathscr{F}$ with the hybrid approach is asymptotically to fix $k_0 = \left\lceil \frac{n}{\nu_0^2} \right\rceil$ variables, where ν_0 is a root of $B_\infty(\nu)$ such that $\nu_0, 0 < \beta_0 \leqslant 1$. The coefficient $\beta_0 = \frac{1}{\nu_0^2}$ is independent of n.*

We show in Table 1 the value of $\beta_0 = \frac{1}{\nu_0^2}$ with respect to several usual sizes of field q. We compare these values with the exact ratio β_0 when $n = 100$ and $n = 200$ (once the parameters are fixed, we can compute exact value β_0^{exact} minimizing the complexity of the hybrid approach). The table shows that our approximation matches well with the expected value.

Table 1: Sample values for β_0 for several field sizes with $\omega = 2.4$. We need less variables to reach the best trade-off when the field is bigger.

q	2^2	2^3	2^4	2^5	2^6	2^8	2^{16}
β_0	0.52	0.35	0.24	0.17	0.12	0.071	0.017
$\beta_0^{\text{exact}}, n = 100$	0.59	0.35	0.25	0.14	0.12	0.08	0.02
$\beta_0^{\text{exact}}, n = 200$	0.55	0.39	0.24	0.17	0.17	0.09	0.02

Note that the the proportion of variables which needs to be fixed tends to 0 when the size of the field increases. This is consistent with the intuition that the exhaustive search becomes less interesting for too big fields.

3.4 Complexity of the Hybrid Approach – An Asymptotic Equivalent

We derive in this part an explicit (asymptotic) equivalent of the hybrid approach complexity. The only element which is missing to get this equivalent is an explicit form of the β_0 discussed in Section 3.3. Table 1 suggests that when q grows, $\beta_0 = \frac{1}{\nu_0^2}$ decreases. This means that $\nu_0 \to \infty$ when $q \to \infty$. This remark combined with Proposition 3.2 leads to the following result.

PROPOSITION 3.3. *Let $\mathscr{F} = \{f_1, \ldots, f_n\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a system of quadratic equations verifying Hypothesis 1. Asymptotically, the best trade-off for solving $\mathscr{F}$ with the hybrid approach is to fix $k_0 = \lceil n\beta_0 \rceil$ variables, with:*

$$\begin{aligned}\beta_0 &= \left(\frac{3\,\omega\log(3)}{6\log(q) + 6\,\omega\log(2) - 4\,\omega - 3\,\omega\log(3)}\right)^2, \\ &= \frac{10.86\,\omega^2}{(4.16\log_2(q) - 3.14\,\omega)^2}\end{aligned}$$

PROOF. Let $B_\infty(\nu)$ be as defined in Proposition 3.2. We get that $B_\infty(\nu) \sim_{\nu\to\infty}$

$$\log(q) - \frac{1}{2}\,\omega\log(3)\,\nu + \omega\left(\log(2) - \frac{2}{3} - \frac{1}{2}\log(3)\right).$$

Let ν_0 be a root of $B_\infty(\nu)$ at infinity (i.e. $\nu \to \infty$). We get:

$$\nu_0 = \frac{6\log(q) + 6\,\omega\log(2) - 4\,\omega - 3\,\omega\log(3)}{3\,\omega\log(3)}. \qquad (10)$$

Then, as $k_0 = \lceil n\beta_0 \rceil = \left\lceil \frac{n}{\nu_0^2} \right\rceil$, we recover the result announced. Note that when q is too small, β_0 becomes greater than one and the approximation is not valid. $\square$

We are now in position to derive the (asymptotical) complexity of the hybrid approach. We use the value of β_0 provided in Proposition 3.3 together with (7) to have an asymptotic of the regularity. It is a multiple of n, and we denote by γ_0 the corresponding factor. Precisely:

$$\gamma_0 = \left(\frac{1+\beta_0}{2} - \sqrt{\beta_0}\right). \qquad (11)$$

Finally, we obtain the asymptotic complexity of the hybrid approach – with the best tradeoff – using the complexity (5). Let $D_0 = 1 - \beta_0 + \gamma_0$, we have $C_{\text{hyb}}(k_0) = C_{\text{hyb}}(\beta_0 n)$

$$\begin{aligned}&\sim \frac{q^{\beta_0 n}}{(\sqrt{2\pi})^\omega} \cdot \left(\frac{(n - \beta_0 n + \gamma_0 n)^{n-\beta_0 n+\gamma_0 n+\frac{1}{2}}}{(n-\beta_0 n)^{n-\beta_0 n+\frac{1}{2}}\,(\gamma_0 n)^{\gamma_0 n+\frac{1}{2}}}\right)^\omega, \\ &\sim \frac{q^{\beta_0 n}}{(\sqrt{2\pi})^\omega} \cdot \frac{1}{(\sqrt{n})^\omega} \cdot \left(\frac{D_0^{n-\beta_0 n+\gamma_0 n+\frac{1}{2}}}{(1-\beta_0)^{n-\beta_0 n+\frac{1}{2}}\,\gamma_0^{\gamma_0 n+\frac{1}{2}}}\right)^\omega, \\ &\sim \frac{q^{\beta_0 n}}{(\sqrt{2\pi n})^\omega} \cdot \left(\frac{D_0}{(1-\beta_0)\gamma_0}\right)^{\frac{\omega}{2}} \cdot \left(\frac{D_0^{D_0}}{(1-\beta_0)^{1-\beta_0}\,\gamma_0^{\gamma_0}}\right)^{\omega n}. \qquad (12)\end{aligned}$$

This leads to:

THEOREM 3.1. *The complexity of the hybrid approach – using the trade-off $k_0 = \lceil \beta_0 n \rceil$ of Proposition 3.3 – is asymptotically equivalent to*

$2^{n\,\omega\left(1.38 - 0.63\,\omega\log_2(q)^{-1}\right)}$, *when $n \to \infty, q \to \infty$ and $\log(q) \ll n$.*

PROOF. From (12) and using the value k_0 in Prop. 3.3:

$$\log_2\left(C_{\text{hyb}}(k_0)\right) \sim nK - \omega\log_2\left(\sqrt{2\pi n}\right) + O(1) \qquad (13)$$

with $K =$

$$\begin{aligned}&\frac{\log_2(q)}{\nu_0^2} + \omega\left(\frac{3}{2} - \frac{1}{2\nu_0^2} - \frac{1}{\nu_0}\right)\log_2\left(\frac{3}{2} - \frac{1}{2\nu_0^2} - \frac{1}{\nu_0}\right) \\ &\quad - \omega\left(1 - \frac{1}{\nu_0^2}\right)\log_2\left(1 - \frac{1}{\nu_0^2}\right) \\ &\quad - \omega\left(\frac{1}{2} + \frac{1}{2\nu_0^2} - \frac{1}{\nu_0}\right)\log_2\left(\frac{1}{2} + \frac{1}{2\nu_0^2} - \frac{1}{\nu_0}\right).\end{aligned}$$

When $q \to \infty$, K tends to

$$\frac{3}{2}\,\omega\log_2(3) - \omega - \frac{1}{4}\,\frac{\omega^2\log_2(3)^2}{\log_2(q)} = 1.38\,\omega - 0.63\,\frac{\omega^2}{\log_2(q)}.$$

The first term in (13) is dominant, so the complexity of the hybrid approach is asymptotically 2^{nK}. $\square$

If $\omega = 2.4$ for instance, the complexity of the hybrid approach is:

$$2^{n\left(3.31 - 3.62\log_2(q)^{-1}\right)}.$$

4. ASYMPTOTIC GAIN OF THE HYBRID APPROACH

The purpose of this part is to quantify the gain of the hybrid approach with respect to a direct approach. We restrict our attention here to the case $m = n$ (i.e. $\alpha = 1$).

The degree of regularity of a square quadratic system of n equations is $n+1$ [8]. Using Stirling's formula in (4):

$$C_{\mathrm{F}_5} \sim \left(\frac{1}{\sqrt{2\pi}} \cdot \frac{(2n+1)^{2n+\frac{3}{2}}}{n^{n+\frac{1}{2}}\,(n+1)^{n+\frac{3}{2}}}\right)^{\omega}.$$

To simplify this expression, we use:

$$\frac{(2n+1)^{2n+\frac{3}{2}}}{(2n)^{2n+\frac{3}{2}}} = \left(1+\frac{1}{2n}\right)^{2n+\frac{3}{2}} \sim e.$$

Thus, $C_{\mathrm{F}_5} \sim$

$$\left(\frac{1}{\sqrt{2\pi}} \cdot \frac{e\,(2n)^{2n+\frac{3}{2}}}{n^{n+\frac{1}{2}}\,e\,n^{n+\frac{3}{2}}}\right)^{\omega} \sim \left(\frac{1}{\sqrt{2\pi}} \cdot \frac{n^{2n+\frac{3}{2}}\,2^{2n+\frac{3}{2}}}{n^{n+\frac{1}{2}}\,n^{n+\frac{3}{2}}}\right)^{\omega}$$

$$\sim \left(\frac{1}{\sqrt{2\pi}} \cdot \frac{2^{2n+\frac{3}{2}}}{n^{\frac{1}{2}}}\right)^{\omega}.$$

Finally:

$$C_{\mathrm{F}_5} \sim \left(\frac{2}{\sqrt{\pi n}}\right)^{\omega} \cdot 2^{2\omega n}. \qquad (14)$$

Let k_0 be as defined in Proposition 3.3. Using (12) and (14), we get that $\frac{C_{\mathrm{F}_5}}{C_{\mathrm{hyb}}(k_0)} \sim \left(\frac{2}{\sqrt{\pi n}}\right)^{\omega} \times$

$$\frac{2^{2\omega n}\,(\sqrt{2\pi n})^{\omega}}{q^{\beta_0 n}} \left(\frac{(1-\beta_0)\,\gamma_0}{1-\beta_0+\gamma_0}\right)^{\frac{\omega}{2}} \left(\frac{(1-\beta_0)^{1-\beta_0}\,\gamma_0^{\gamma_0}}{(1-\beta_0+\gamma_0)^{1-\beta_0+\gamma_0}}\right)^{\omega n}.$$

This last expression can be written as follows:

$$\left(2\sqrt{2}\right)^{\omega} \cdot \left(\frac{(1-\beta_0)\,\gamma_0}{1-\beta_0+\gamma_0}\right)^{\frac{\omega}{2}} \cdot \left(\frac{1}{q^{\beta_0}}\left(2^2 \cdot \frac{(1-\beta_0)^{1-\beta_0}\,\gamma_0^{\gamma_0}}{(1-\beta_0+\gamma_0)^{1-\beta_0+\gamma_0}}\right)^{\omega}\right)^{n}.$$

As a consequence:

$$\frac{C_{\mathrm{F}_5}}{C_{\mathrm{hyb}}(k_0)} \sim \frac{1}{q^{\beta_0 n}}\left(2^2 \cdot \frac{(1-\beta_0)^{1-\beta_0}\,\gamma_0^{\gamma_0}}{(1-\beta_0+\gamma_0)^{1-\beta_0+\gamma_0}}\right)^{\omega n}. \qquad (15)$$

This corresponds to the asymptotic gain of the hybrid approach. To simplify our notations, we denote by $Q = \log_2\left(\frac{C_{\mathrm{F}_5}}{C_{\mathrm{hyb}}(k_0)}\right)$ the logarithm of the gain. It holds that $Q \sim nC$, with:

$$C = -\beta_0 \log_2(q) + 2\,\omega \log_2(2) + \omega \log_2\left(\frac{(1-\beta_0)^{1-\beta_0}\,\gamma_0^{\gamma_0}}{(1-\beta_0+\gamma_0)^{1-\beta_0+\gamma_0}}\right).$$

Note that C does not depend on n. We replace β_0 and γ_0 by their respective values obtained from Prop. 3.3 and equation (11). To have an approximation of this gain, one can compute an asymptotic expansion of C when $q \to \infty$. Using the logarithmic in base 2:

$$C \sim 3\,\omega - \frac{3}{2}\,\omega \log_2(3) = 0.62\,\omega. \qquad (16)$$

This allows to state the following:

THEOREM 4.1. *Let $\mathscr{F} = \{f_1, \ldots, f_n\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be quadratic equations verifying Hypothesis 1. When $n \to \infty$, $q \to \infty$ and as long as $n \gg \log_2(q)$, the gain of the hybrid approach compared to a direct Gröbner basis approach is asymptotically $2^{0.62\,\omega n}$.*

Theorem 4.1 gives a trend of the asymptotic gain. It shows the overall efficiency of the hybrid approach compared to the simple Gröbner basis approach. For $\omega = 2.4$, we get a speed-up of $2^{1.49n}$ as stated in the abstract.

On the other hand, the actual gain can be more precisely computed with explicit values of C_{hyb}, the best trade-off, and C_{F_5}). We compare the real gain with several of our asymptotic estimations for fields of size $q = 2, 16, 256, 2^{16}, 2^{32}$ using $\omega = 2.4$. Each figure (Fig. 1 to 5) has four curves, except when $q \leqslant 13$, where the approximation of Proposition 3.3 is not relevant. – The theoretical gain (plain line) obtained from the explicit complexity of C_{F_5} (4) and the best trade-off as the minimum of Proposition 2.1 for all $k, 0 \leqslant k \leqslant n$.

– The gain when $n \to \infty$ (dashed line) obtained from (16) and the trade-off is computed with Proposition 3.1.

– The gain when $n \to \infty$ with k_0 from Proposition 3.3 (loosely dashed line) obtained from (16) (relevant for $q > 13$).

– The asymptotic gain when $n \to \infty$ and $q \to \infty$ (dotted line) of Theorem 4.1.

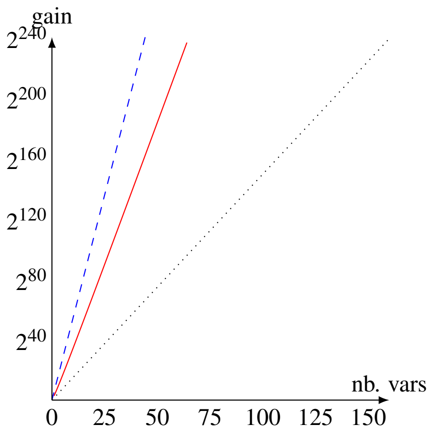

Figure 1: Gain when solving a system over $\mathbb{F}_2$.

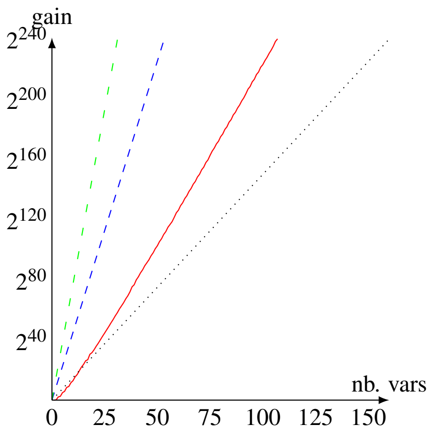

Figure 2: Gain when solving a system over $\mathbb{F}_{16}$.

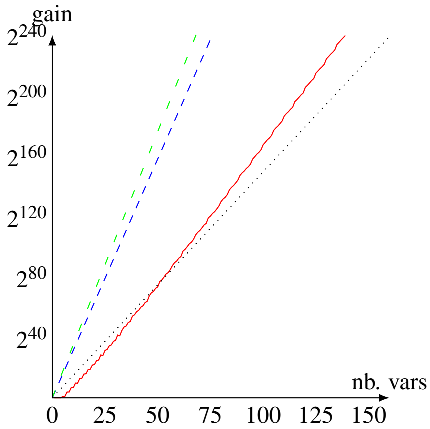

Figure 3: Gain when solving a system over $\mathbb{F}_{2^8}$.

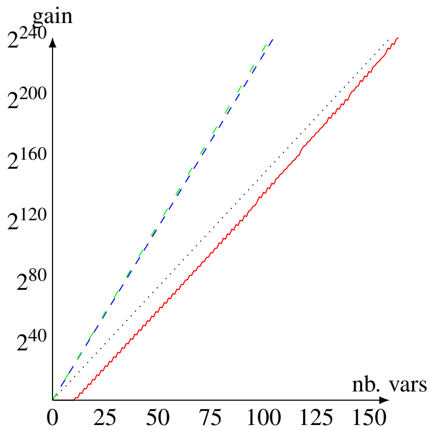

Figure 4: Gain when solving a system over $\mathbb{F}_{2^{16}}$.

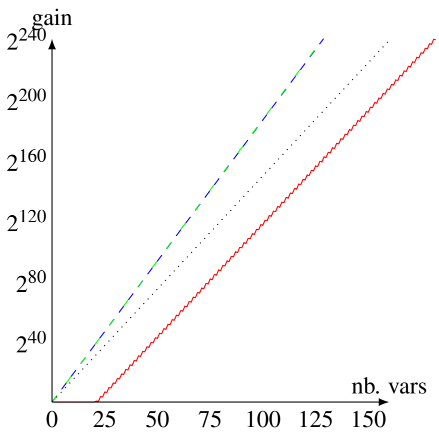

Figure 5: Gain when solving a system over $\mathbb{F}_{2^{32}}$.

As expected, the gain becomes more accurate as q grows (Fig. 1 to 3). When n is not big enough compared to q, it becomes less accurate (Fig. 5).

Asymptotically, the hybrid approach is then always better than a direct solving. Eventually, when q is too big (with respect to n), the cost of an exhaustive search, even in one single variable, will be too expensive compared to Gröbner basis computation.

Acknowledgments. We would like to thank the referees for their meaningful comments. The work described in this paper has been supported in part by the European Commission through the ICT program under contract ICT-2007-216676 ECRYPT II. The authors were also supported in part by the french ANR under the Computer Algebra and Cryptography (CAC) project ANR-09-JCJCJ-0064-01 and the High-Performance Algebraic Computing (HPAC) project ANR-2011-BS02-013-04.

5. REFERENCES

[1] M. Albrecht, J.-C. Faugère, P. Farshim, and L. Perret. Polly cracker, revisited. In D. Lee and X. Wang, editors, *Advances in Cryptology Asiacrypt 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 179–196. Springer Berlin / Heidelberg, 2011.

[2] G. Ars, J.-C. Faugère, H. Imai, M. Kawazoe, and M. Sugita. Comparison between xl and gröbner basis algorithms. In P. J. Lee, editor, *ASIACRYPT*, volume 3329 of *Lecture Notes in Computer Science*, pages 338–353. Springer, 2004.

[3] D. Augot, J.-C. Faugère, and L. Perret. Foreword. *J. Symb. Comput.*, 44(12):1605–1607, 2009.

[4] M. Bardet. *Études des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, Université Paris 6, Décembre 2004.

[5] M. Bardet, J.-C. Faugère, and B. Salvy. Complexity study of Gröbner basis computation. Technical report, INRIA, 2002. `http://www.inria.fr/rrrt/rr-5049.html`.

[6] M. Bardet, J.-C. Faugère, and B. 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, 2004.

[7] M. Bardet, J.-C. Faugère, B. Salvy, and P.-J. Spaenlehauer. On the complexity of solving quadratic boolean systems. *CoRR*, abs/1112.6263, 2011.

[8] M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *The Effective Methods in Algebraic Geometry Conference – MEGA 2005*, pages 1–14, 2005.

[9] L. Bettale, J.-C. Faugère, and L. Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, volume 3(issue 3):177–197, 2009.

[10] C. Bouillaguet, H.-C. Chen, C.-M. Cheng, T. Chou, R. Niederhagen, A. Shamir, and B.-Y. Yang. Fast exhaustive search for polynomial systems in f_2. In S. Mangard and F.-X. Standaert, editors, *CHES*, volume 6225 of *Lecture Notes in Computer Science*, pages 203–218. Springer, 2010.

[11] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.

[12] B. Buchberger. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41(3-4):475–511, 2006.

[13] B. Buchberger, G. E. Collins, R. G. K. Loos, and R. Albrecht. Computer algebra symbolic and algebraic computation. *SIGSAM Bull.*, 16(4):5–5, 1982.

[14] C. Cid, S. Murphy, and M. J. B. Robshaw. *Algebraic aspects of the advanced encryption standard*. Springer, 2006.

[15] N. Courtois, L. Goubin, and J. Patarin. SFLASHv3, a fast asymmetric signature scheme. available at

http://eprint.iacr.org/2003/211.

[16] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Y. Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 267–287. Springer, 2002.

[17] N. T. Courtois and G. V. Bard. Algebraic cryptanalysis of the data encryption standard. In *Cryptography and Coding '07*, volume 4887 of *Lecture Notes in Computer Science*, pages 152–169. Springer, 2007.

[18] I. Dinur and A. Shamir. Cube attacks on tweakable black box polynomials. In A. Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 278–299. Springer, 2009.

[19] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139:61–88, June 1999.

[20] J.-C. 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*, pages 75–83. ACM Press, 2002.

[21] J.-C. Faugère, F. L. dit Vehel, and L. Perret. Cryptanalysis of minrank. In D. Wagner, editor, *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 280–296. Springer, 2008.

[22] J.-C. Faugère, P. M. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *J. Symb. Comput.*, 16(4):329–344, 1993.

[23] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. In *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2003.

[24] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic cryptanalysis of mceliece variants with compact keys. In *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 279–298. Springer, 2010.

[25] J.-C. Faugère, L. Perret, C. Petit, and G. Renault. Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Field. In *Proceedings of Eurocrypt 2012*, Lecture Notes in Computer Science, pages 1–15. Springer Verlag, 2012.

[26] R. Fröberg. An inequality for Hilbert series of graded algebras. *Math. Scand.*, 56(2):117–144, 1985.

[27] S. Gao, Y. Guan, and F. Volny. A new incremental algorithm for computing groebner bases. In W. Koepf, editor, *ISSAC*, pages 13–19. ACM, 2010.

[28] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman and Company, 1979.

[29] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced oil and vinegar signature schemes. In *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer, 1999.

[30] A. Kipnis and A. Shamir. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

[31] A. Kipnis and A. Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In M. J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

[32] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in Cryptology – EUROCRYPT '88*, volume 330 of *Lecture Notes in Computer Science*, pages 419–453. Springer, 1988.

[33] J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

[34] K. Sakumoto, T. Shirai, and H. Hiwatari. Public-key identification schemes based on multivariate quadratic polynomials. In P. Rogaway, editor, *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 706–723. Springer, 2011.

[35] M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso. *Gröbner Bases, Coding, and Cryptography*. Springer, 2009.

[36] M. Sugita, M. Kawazoe, L. Perret, and H. Imai. Algebraic cryptanalysis of 58-round SHA-1. In *Fast Software Encryption*, volume 4593 of *Lecture Notes in Computer Science*, pages 349–365. Springer, 2007.

[37] 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/.

[38] B.-Y. Yang and J.-M. Chen. Theoretical analysis of xl over small fields. In H. Wang, J. Pieprzyk, and V. Varadharajan, editors, *ACISP*, volume 3108 of *Lecture Notes in Computer Science*, pages 277–288. Springer, 2004.

[39] B.-Y. Yang, J.-M. Chen, and N. Courtois. On asymptotic security estimates in xl and gröbner bases-related algebraic cryptanalysis. In J. Lopez, S. Qing, and E. Okamoto, editors, *ICICS*, volume 3269 of *Lecture Notes in Computer Science*, pages 401–413. Springer, 2004.

APPENDIX

Table 2: Sample values for β_0 depending on several values of α and q with $\omega = 2.4$. An entry is empty when there is no positive solution (i.e. best trade-off is $k = 0$).

q	2^2	2^3	2^4	2^5	2^6	2^8	2^{16}
β_0 ($\alpha = 1$)	0.52	0.35	0.24	0.17	0.12	0.071	0.017
β_0 ($\alpha = 1.1$)	0.47	0.29	0.17	0.087	0.036	–	–
β_0 ($\alpha = 1.25$)	0.40	0.19	0.052	–	–	–	–
β_0 ($\alpha = 1.5$)	0.28	0.028	–	–	–	–	–
β_0 ($\alpha = 1.75$)	0.16	–	–	–	–	–	–
β_0 ($\alpha = 2$)	0.042	–	–	–	–	–	–
β_0 ($\alpha = 3$)	–	–	–	–	–	–	–
β_0 ($\alpha = 4$)	–	–	–	–	–	–	–
β_0 ($\alpha = 5$)	–	–	–	–	–	–	–