# A variant of the F4 algorithm

Antoine Joux[1,2] and Vanessa Vitse[2]

[1] Direction Générale de l'Armement (DGA)
[2] Université de Versailles Saint-Quentin, Laboratoire PRISM, 45 av. des États-Unis, 78035 Versailles cedex, France
antoine.joux@m4x.org vanessa.vitse@prism.uvsq.fr

**Abstract.** Algebraic cryptanalysis usually requires to find solutions of several similar polynomial systems. A standard tool to solve this problem consists of computing the Gröbner bases of the corresponding ideals, and Faugère's F4 and F5 are two well-known algorithms for this task. In this paper, we present a new variant of the F4 algorithm which is well suited to algebraic attacks of cryptosystems since it is designed to compute Gröbner bases of a set of polynomial systems having the same shape. It is faster than F4 as it avoids all reductions to zero, but preserves its simplicity and its computation efficiency, thus competing with F5.

**Key words:** Gröbner basis, F4, F5, multivariate cryptography, algebraic cryptanalysis

## 1 Introduction

The goal of algebraic cryptanalysis is to break cryptosystems by using mathematical tools coming from symbolic computation and modern algebra. More precisely, an algebraic attack can be decomposed in two steps: first the cryptosystem and its specifics have to be converted into a set of multivariate polynomial equations, then the solutions of the obtained polynomial system have to be computed. The security of a cryptographic primitive thus strongly relies on the difficulty of solving the associated polynomial system. These attacks have been proven to be very efficient for both public key or symmetric cryptosystems and stream ciphers (see [1] for a thorough introduction to the subject).

In this article, we focus on the polynomial system solving part. It is well known that this problem is very difficult (NP-hard in general). However, for many instances coming from algebraic attacks, the resolution is easier than in the worst-case scenario. Gröbner bases, first introduced in [5], are a fundamental tool for tackling this problem. Historically, one can distinguish two families of Gröbner basis computation algorithms: the first one consists of developments of Buchberger's original algorithm [7, 13, 14, 18], while the second can be traced back to the theory of elimination and resultants and relies on Gaussian elimination of Macaulay matrices [9, 23–25]. Which algorithm to use depends of the shape and properties of the cryptosystem and its underlying polynomial system (base field, degrees of the polynomials, number of variables, symmetries...).

Faugère's F4 algorithm [13] combines ideas from both families. It is probably the most efficient installation of Buchberger's original algorithm, and uses Gaussian elimination to speed up the time-consuming step of "critical pair" reductions. It set new records in Gröbner basis computation when it was published a decade ago, and its implementation in Magma [4] is still considered as a major reference today. However, F4 shares the main drawback of Buchberger's algorithm, namely, it spends a lot of time computing useless reductions. This issue was addressed by Faugère's next algorithm, F5 [14], which first rose to fame with the cryptanalysis of the HFE Challenge [15]. Since then, it has been successfully used to break several other cryptosystems (e.g. [3, 16]), increasing considerably the popularity of algebraic attacks. It is often considered as the most efficient algorithm for computing Gröbner bases over finite fields and its remarkable performances are for the main part attributable to the use of an elaborate criterion. Indeed, the F5 criterion allows to skip much more unnecessary critical pairs than the classical Buchberger's criteria [6]; actually it eliminates a

priori all reductions to zero under the mild assumption that the system forms a semi-regular sequence [2]. Nevertheless, this comes at the price of degraded performances in the reduction step: the polynomials considered in the course of the F5 algorithm are "top-reduced", but their tails are left almost unreduced because many reductions are forbidden for "signature" compatibility conditions.

We propose in this article another method that, by means of a precomputation, allows to avoid all reductions to zero in the F4 algorithm. The proposed method does not work in all situations, but is well suited to the context of algebraic attacks of cryptosystems; the precomputation overhead is largely compensated by the efficiency of the F4 reduction step, yielding theoretically better performances than F5. This new algorithm stems from the observation that in many instances, one has to compute Gröbner bases for numerous polynomial systems that have the same shape, and whose coefficients are either random or depend of a relatively small number of parameters. Thus it is possible to extract from a first F4 execution, a list of relevant critical pairs that will be used for the following computations. Of course, there is no reason why this should work for all subsequent systems, but we can estimate the probability of failure, which is usually very small. This variant of F4 has already been briefly mentioned in [19], where it was applied to the discrete logarithm problem on elliptic curves; it is detailed here for the first time.

The paper is organized as follows. After recalling the basic structure of Buchberger-type algorithms, we explain in section 2 how to adapt it to the context of several systems of the same shape. We then give detailed pseudo-code of our variant of F4, which consists of the two routines `F4Precomp` and `F4Remake`, for the first precomputation and the subsequent iterations respectively. A complete analysis is done in section 3; in particular, we provide a mathematical frame for the otherwise imprecise notion of "similar looking systems" and derive probability estimates for the correctness of our algorithm, depending on the type of the system and the size of the base field. We also compare the complexities of our variant and of F5, and explain when it is better to use our algorithm. The last section is devoted to applications: the first example is the index calculus method of [19] and is a typical case where our algorithm outperforms F4 and F5. We then show how it fits into the hybrid approach of [3] and consider the example of the cryptanalysis of the UOV signature scheme [21]. The next example is provided by the Kipnis-Shamir attack on the MinRank problem: we compare our results to those of [16]. Finally, we evaluate the performances of our F4 variant on the classical `Katsura` benchmarks.

## 2 The F4 variant

### 2.1 Description of the algorithm

We begin by recalling the standard characterization of Gröbner bases:

**Theorem 1 ([7])** *A family $G = \{g_1, \ldots, g_s\}$ in $\mathbb{K}[X_1, \ldots, X_n]$ is a Gröbner basis if and only if for all $1 \leq i < j \leq s$, the remainder of $S(g_i, g_j)$ on division by $G$ is zero, where $S(g_i, g_j)$ is the S-polynomial of $g_i$ and $g_j$: $S(g_i, g_j) = \dfrac{LM(g_i) \vee LM(g_j)}{LT(g_i)} g_i - \dfrac{LM(g_i) \vee LM(g_j)}{LT(g_j)} g_j$.*

It is straightforward to adapt this result into the Buchberger's algorithm [7], which outputs a Gröbner basis of an ideal $I = \langle f_1, \ldots, f_r \rangle$: one computes iteratively the remainder by $G$ of every possible S-polynomials and appends this remainder to $G$ whenever it is different from zero. In the following, we will rather work with critical pairs instead of S-polynomials: the critical pair of two polynomials $f_1$ and $f_2$ is defined as the tuple $(lcm, u_1, f_1, u_2, f_2)$ where $lcm = LM(f_1) \vee LM(f_2)$ and $u_i = \frac{lcm}{LM(f_i)}$.

The reduction of critical pairs is by far the biggest time-consuming part of the Buchberger's algorithm. The main idea of Faugère's F4 algorithm is to use linear algebra to simultaneously reduce a large number of

pairs. At each iteration step, a Macaulay-style matrix is constructed, whose columns correspond to monomials and rows to polynomials. This matrix contains the products $(u_i f_i)$ coming from the selected critical pairs (classically, all pairs with the lowest total degree lcm, but other selection strategies are possible) and also all polynomials involved in their reductions, which are determined during the preprocessing phase. By computing the reduced row echelon form of this matrix, we obtain the reduced S-polynomials of all pairs considered. This algorithm, combined with an efficient implementation of linear algebra, yields very good results.

As mentioned in the introduction, F4 has the drawback of computing many useless reductions to zero, even when the classical criteria of Buchberger [6] are taken into account. But when one has to compute several Gröbner bases of similar polynomial systems, it is possible to avoid, in most cases, all reductions to zero by means of a precomputation on the first system. Here is the outline of our F4 variant:

1. For precomputation purposes, run a standard F4 algorithm on the first system, with the following modifications:
   - At each iteration, store the list of all polynomial multiples $(u_i, f_i)$ coming from the critical pairs.
   - During the row echelon computing phase, reductions to zero correspond to linear dependency relations between the rows of the matrix; for each such relation, remove a multiple $(u_i, f_i)$ from the stored list.
2. For each subsequent system, run a F4 computation with the following modifications:
   - Do not maintain nor update a queue of untreated pairs.
   - At each iteration, instead of selecting pairs from the queue, pick directly from the previously stored list all the relevant multiples $(u_i, f_i)$.

### 2.2 Pseudo-code

We now give the detailed pseudo-code of the `F4Precomp` algorithm which performs the precomputation, and of the `F4Remake` algorithm which is used for the subsequent systems.

**The precomputation**

Given a family of polynomials $\{f_1, \ldots, f_r\}$, the `F4Precomp` algorithm computes for each iteration step of the classical F4 algorithm, the list of polynomial multiples that will be used by `F4Remake` on subsequent computations. This algorithm follows very closely [13], with the following additional features:

- A list $L$ of lists of couples is introduced; at the end of the $i$-th main iteration, $L[i]$ contains the desired list of polynomial multiples for that step. Each polynomial multiple is represented by a couple $(m, n)$, where $m$ is a monomial and $n$ is the index of the polynomial in a global list $G$ (this list $G$ will be progressively reconstructed by `F4Remake`). In the same way, a list $L_{tmp}$ is used to temporary store these couples.
- Instead of just computing the reduced row echelon form $M'$ of the matrix $M$, we also compute an auxiliary matrix $A$ such that $AM = M'$. If reductions to zero occur, then the bottom part of $M'$ is null and the corresponding bottom part of $A$ gives the linear dependencies between the rows of $M$. This information is exploited in lines 27 to 36, in order to remove from the temporary list $L_{tmp}$ the useless multiples before copy in $L[step]$. Actually, only the bottom-left part $A'$ of $A$ is of interest: it contains the linear dependencies between the rows of $M$ coming from the critical pairs, modulo those coming from the preprocessing. It is clear that with each dependency relation, one polynomial multiple can be removed, but some care must be taken in this choice. To do so, the row echelon form $\tilde{A}$ of $A'$ is then computed and the polynomial multiples corresponding to the pivots of $\tilde{A}$ are removed. Among the remaining polynomial multiples, those whose leading monomial is now unique can also be removed.

Apart from these modifications, the pseudo-code is basically the F4 algorithm with Gebauer and Möller installation of the BuchBerger's criteria (`Update` subroutine) [18]. The only notable change concerns the implementation of the `Simplify` procedure: instead of searching through all the former matrices and their row echelon forms for the adequate simplification as in [13], we introduce an array $TabSimplify$ which contains for each polynomial $f$ in the basis a list of couple of the form $(m, g) \in T \times \mathbb{K}[\underline{X}]$, meaning that the

product $mf$ can be simplified into the more reduced polynomial $g$. This array is updated after the reduced row echelon form is computed (lines 14 to 24 of `Postprocessing`)

**Alg. 1** F4Precomp

INPUT : $f_1, \ldots, f_r \in \mathbb{K}[\underline{X}]$
OUTPUT : a list of lists of couples $(m, n) \in T \times \mathbb{N}$

1. $G \leftarrow [\,],\ G_{min} \leftarrow \emptyset,\ P \leftarrow \emptyset, TabSimplify \leftarrow [\,], L \leftarrow [\,]$
2. **for** $i = 1$ to $r$ **do**
3. $\quad G[i] \leftarrow f_i$
4. $\quad TabSimplify[i] \leftarrow [(1, f_i)]$
5. $\quad Update(f_i)$
6. **end for**
7. $step = 1$
8. **while** $P \neq \emptyset$ **do**
9. $\quad P_{sel} \leftarrow Sel(P)$
10. $\quad F \leftarrow [\,], LM(F) \leftarrow \emptyset, T(F) \leftarrow \emptyset, L[step] \leftarrow [\,], L_{tmp} \leftarrow [\,]$
11. $\quad$ **for all** $pair = (lcm, t_1, g_1, t_2, g_2) \in P_{sel}$ **do**
12. $\quad\quad$ **for** $k = 1$ to $2$ **do**
13. $\quad\quad\quad ind \leftarrow index(g_k, G)$
14. $\quad\quad\quad$ **if** $(t_k, ind) \notin L_{tmp}$ **then**
15. $\quad\quad\quad\quad Append(L_{tmp}, (t_k, ind))$
16. $\quad\quad\quad\quad f \leftarrow Simplify(t_k, ind)$
17. $\quad\quad\quad\quad Append(F, f)$
18. $\quad\quad\quad\quad LM(F) \leftarrow LM(F) \cup \{LM(f)\}$
19. $\quad\quad\quad\quad T(F) \leftarrow T(F) \cup \{m \in T : m \text{ monomial of } f\}$
20. $\quad\quad\quad$ **end if**
21. $\quad\quad$ **end for**
22. $\quad$ **end for**
23. $\quad Preprocessing(F, T(F), LM(F))$
24. $\quad M \leftarrow$ matrix whose rows are the polynomials in $F$
25. $\quad (M'|A) \leftarrow ReducedRowEchelonForm(M|I_{\#F})\ (\Rightarrow AM = M')$
26. $\quad rk \leftarrow Postprocessing(M', LM(F))$
27. $\quad$ **if** $rk < \#F$ **then**
28. $\quad\quad A' \leftarrow A[rk + 1..\#F][1..\#L_{tmp}]$
29. $\quad\quad \tilde{A} \leftarrow ReducedRowEchelonForm(A')$
30. $\quad\quad C \leftarrow \{c \in \{1, \ldots, \#L_{tmp}\} : c \text{ is not a column number of a pivot in } \tilde{A}\}$
31. $\quad\quad$ **for** $j \in C$ **do**
32. $\quad\quad\quad$ **if** $\exists k \in C$ such that $k \neq j$ and $LM(F[k]) = LM(F[j])$ **then**
33. $\quad\quad\quad\quad Append(L[step], L_{tmp}[j])$
34. $\quad\quad\quad$ **end if**
35. $\quad\quad$ **end for**
36. $\quad$ **end if**
37. $\quad step \leftarrow step + 1$
38. **end while**
39. **return** $L$

In the pseudo-code, the following variables are supposed to be global: $G$, a list of polynomials that forms a basis of $\langle f_1, \ldots, f_r \rangle$; $G_{min}$, a set of polynomials which is the minimalized version of $G$; $TabSimplify$, an array of lists of couples used for the simplification of polynomials multiples; $P$, a queue of yet untreated critical pairs. The function $Sel$ on line 9 is a selection function, whose expression depends on the chosen strategy; according to Faugère's recommendations, selecting all pairs of lowest total degree lcm (normal strategy) usually yields the best performances. The notation $index(g, G)$ stands for the integer $i$ such that $G[i] = g$,

and the function $pair(f_1, f_2)$ outputs the critical pair $(lcm, u_1, f_1, u_2, f_2)$. Finally, *ReducedRowEchelonForm* computes as expected the reduced row echelon form of its input matrix. We stress that great care should be taken in the implementation of this last function since almost all the execution time of the algorithm is spent in it. Note that the test on line 21 in `Update` is only necessary during the initialisation phase of `F4Precomp` (line 5).

**Alg. 2** Update

INPUT : $f \in \mathbb{K}[\underline{X}]$

1. **for all** $pair = (lcm, t_1, g_1, t_2, g_2) \in P$ **do**
2. **if** $(LM(f) \vee LM(g_1)$ divides strictly $lcm)$ AND $(LM(f) \vee LM(g_2)$ divides strictly $lcm)$ **then**
3. $P \leftarrow P \setminus \{pair\}$
4. **end if**
5. **end for**
6. $P_0 \leftarrow \emptyset, P_1 \leftarrow \emptyset, P_2 \leftarrow \emptyset$
7. **for all** $g \in G_{min}$ **do**
8. **if** $LM(f) \wedge LM(g) = 1$ **then**
9. $P_0 \leftarrow P_0 \cup pair(f, g)$
10. **else**
11. $P_1 \leftarrow P_1 \cup pair(f, g)$
12. **end if**
13. **end for**
14. **for all** $pair = (lcm, t_1, g_1, t_2, g_2) \in P_1$ **do**
15. $P_1 \leftarrow P_1 \setminus \{pair\}$
16. **if** $\nexists pair' = (lcm', t_1', g_1', t_2', g_2') \in P_0 \cup P_1 \cup P_2$ such that $lcm' | lcm$ **then**
17. $P_2 \leftarrow P_2 \cup \{pair\}$
18. **end if**
19. **end for**
20. $P \leftarrow P \cup P_2$
21. **if** $\nexists g \in G_{min}$ such that $LM(g) | LM(f)$ **then**
22. **for all** $g \in G_{min}$ **do**
23. **if** $LM(f) | LM(g)$ **then**
24. $G_{min} \leftarrow G_{min} \setminus \{g\}$
25. **end if**
26. $G_{min} \leftarrow G_{min} \cup \{f\}$
27. **end for**
28. **end if**

**Alg. 3** Simplify

INPUT : $t \in T, ind \in \mathbb{N}$

OUTPUT : $p \in \mathbb{K}[\underline{X}]$

1. **for** $(m, f) \in TabSimplify[ind]$ (from last to first) **do**
2. **if** $m = t$ **then**
3. **return** $f$
4. **else**
5. **if** $m | t$ **then**
6. $Append\left(TabSimplify[ind], \left(m, \frac{t}{m} f\right)\right)$
7. **return** $\frac{t}{m} f$
8. **end if**
9. **end if**
10. **end for**

**Alg. 4** Preprocessing

INPUT : $F, T(F), LM(F)$

**while** $T(F) \neq Done$ **do**
  $m \leftarrow \max(T(F) \setminus Done)$
  $Done \leftarrow Done \cup \{m\}$
  **for all** $g \in G_{min}$ **do**
    **if** $LM(g)|m$ **then**
      $g' \leftarrow Simplify\left(\frac{m}{LM(g)}, index(g, G)\right)$
      $Append(F, g')$
      $LM(F) \leftarrow LM(F) \cup \{m\}$
      $T(F) \leftarrow T(F) \cup \{m' \in T : m' \text{ monomial of } g'\}$
      **break**
    **end if**
  **end for**
**end while**

**Alg. 5** Postprocessing

INPUT : a matrix $M$ in reduced row echelon form with $\#F$ lines and an ordered set of monomials $LM(F)$
OUTPUT : the rank of the matrix $M$

**for** $i = 1$ to $\#F$ **do**
  $f \leftarrow M[i]$
  **if** $f = 0$ **then**
    **break**
  **end if**
  **if** $LM(f) \notin LM(F)$ **then**
    $Append(G, f)$
    $Update(f)$
    $TabSimplify[\#G] \leftarrow [(1, f)]$
  **else**
    **for** $g \in G_{min}$ **do**
      $ind \leftarrow index(g, G)$
      **if** $LM(g)|LM(f)$ **then**
        **for** $j = 1$ to $\#TabSimplify[ind]$ **do**
          **if** $TabSimplify[ind][j] = \left(\frac{LM(f)}{LM(g)}, .\right)$ **then**
            $TabSimplify[ind][j] = \left(\frac{LM(f)}{LM(g)}, f\right)$
            **break**
          **end if**
        **end for**
        **if** $j > \#TabSimplify[ind]$ **then**
          $Append\left(TabSimplify[ind], \left(\frac{LM(f)}{LM(g)}, f\right)\right)$
        **end if**
      **end if**
    **end for**
  **end if**
**end for**
**return** $i - 1$

**F4Remake**

The `F4Remake` algorithm uses the same routines `Simplify`, `Preprocessing` and `Postprocessing`. Since it no longer uses critical pairs, the subroutine `Update` can be greatly simplified and is replaced by `Update2`.

**Alg. 6** F4Remake

INPUT : $f_1, \ldots, f_r \in \mathbb{K}[\underline{X}]$, a list $L$ of lists of couples $(m, n) \in T \times \mathbb{N}$
OUTPUT : $G_{min}$, the reduced minimal Gröbner basis of $f_1, \ldots, f_r$

1. $G \leftarrow [\,],\ G_{min} \leftarrow \emptyset, TabSimplify \leftarrow [\,]$
2. **for** $i = 1$ to $r$ **do**
3. $\quad G[i] \leftarrow f_i$
4. $\quad TabSimplify[i] \leftarrow [(1, f_i)]$
5. $\quad Update2(f_i)$
6. **end for**
7. **for** $step = 1$ to $\#L$ **do**
8. $\quad F \leftarrow [\,],\ LM(F) \leftarrow \emptyset,\ T(F) \leftarrow \emptyset$
9. $\quad$ **for all** $(m, n) \in L[step]$ **do**
10. $\quad\quad$ **if** $n > \#G$ **then**
11. $\quad\quad\quad$ computation fails ! **exit**
12. $\quad\quad$ **end if**
13. $\quad\quad Simplify(m, n),\ Append(F, f)$
14. $\quad\quad LM(F) \leftarrow LM(F) \cup \{LM(f)\}$
15. $\quad\quad T(F) \leftarrow T(F) \cup \{m \in T : m \text{ monomial of } f\}$
16. $\quad$ **end for**
17. $\quad Preprocessing(F, T(F), LM(F))$
18. $\quad M \leftarrow$ matrix whose rows are the polynomials in $F$
19. $\quad M' \leftarrow ReducedRowEchelonForm(M)$
20. $\quad Postprocessing(M', LM(F))$
21. **end for**
22. **return** $InterReduce(G_{min})$

**Alg. 7** Update2

INPUT : $f \in \mathbb{K}[\underline{X}]$

1. **if** $\nexists g \in G_{min}$ such that $LM(g) | LM(f)$ **then**
2. $\quad$ **for all** $g \in G_{min}$ **do**
3. $\quad\quad$ **if** $LM(f) | LM(g)$ **then**
4. $\quad\quad\quad G_{min} \leftarrow G_{min} \setminus \{g\}$
5. $\quad\quad$ **end if**
6. $\quad\quad G_{min} \leftarrow G_{min} \cup \{f\}$
7. $\quad$ **end for**
8. **end if**

## 3 Analysis of the algorithm and complexity

### 3.1 Similar systems

Our algorithm is designed to be applied on many systems of the "same shape". If $\{f_1, \ldots, f_r\}$ and $\{f'_1, \ldots, f'_r\}$ are two similarly-looking polynomial systems, we want to estimate the probability that our algorithm com-

putes the Gröbner basis of the second system, the precomputation having been done with the first system. This requires some more precise definitions.

**Definition 2** *A generic polynomial $F$ of degree $d$ in $n$ variables $X_1, \ldots, X_n$ is a polynomial with coefficients in $\mathbb{K}[\{Y_{i_1,\ldots,i_n}\}_{i_1+\ldots+i_n\leq d}]$ of the form $F = \sum_{i_1+\ldots+i_n\leq d} Y_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$.*

A generic polynomial is thus a polynomial in which each coefficient is a distinct variable. Such polynomials are interesting to study because a system of random polynomials $f_1, \ldots, f_r$ (i.e. such that each coefficient is random) of total degree $d_1, \ldots, d_r$ respectively, is expected to behave like the corresponding system of generic polynomials.

Let $F_1, \ldots, F_r$ be a system of generic polynomials. If we consider $F_i$ as an element of $\mathbb{K}(\underline{Y})[\underline{X}]$, we can compute the Gröbner basis of this system with the F4 algorithm, at least theoretically (in practice, the rational fraction coefficients will likely become extremely large). Now let $f_1, \ldots, f_r$ be a random system with $\deg(f_i) = \deg(F_i)$. We say that $f_1, \ldots, f_r$ behaves generically if we encounter the same number of iterations as with $F_1, \ldots, F_r$ during the computation of its Gröbner basis using F4, and if the same number of new polynomials with the same leading monomials are generated at each step of the algorithm. We will now translate this condition algebraically. Assume that the system $f_1, \ldots, f_r$ behaves generically until the $(i-1)$-th step; this implies in particular that the critical pairs involved at step $i$ for both systems are similar, in the following sense: $(lcm, u_1, p_1, u_2, p_2)$ is similar to $(lcm', u_1', p_1', u_2', p_2')$ if $LM(p_1) = LM(p_1')$ and $LM(p_2) = LM(p_2')$ (so that $u_i = u_i'$ and $lcm = lcm'$).

Let $M_g$ be the matrix of polynomial multiples constructed by F4 at step $i$ for the generic system, and $M$ be the one for $f_1, \ldots, f_r$. It is possible that after the preprocessing $M$ is smaller than $M_g$, but for the purpose of our discussion, we may assume that the missing polynomial multiples are added to $M$; the corresponding rows will have no effect whatsoever later in the algorithm. Thus the $k$-th rows of $M$ and $M_g$, seen as polynomials, have identical leading monomial; we note $s$ the number of distinct leading monomials in $M$ (or $M_g$). If we compute the reduced row echelon form of $M_g$, up to a well-chosen permutation of columns we obtain

$$\tilde{M_g} = \left(\begin{array}{c|c} I_{rk} & A \\ \hline 0 & 0 \end{array}\right)$$

Using the same transformations on $M$ with adapted coefficients, we obtain a matrix

$$\tilde{M} = \left(\begin{array}{c|c|c} I_s & C & \\ \hline 0 & B & A' \\ \hline 0 & 0 & \end{array}\right)$$

where $B$ is a square matrix of size $rk - s$. Then the system $f_1, \ldots, f_r$ behaves generically at step $i$ if and only if this matrix $B$ is invertible. Finally, we obtain that the system behaves generically during the course of the F4 algorithm if at each step, the corresponding matrix $B$ is invertible.

Heuristically, since the system is random, we will assume that these matrices $B$ are random. This hypothesis will allow us to give estimates for the probability that a system behaves generically, using the following easy lemma:

**Lemma 3** *Let $M = (m_{ij}) \in \mathcal{M}_n(\mathbb{F}_q)$ be a random square matrix, i.e. such that the coefficients $m_{ij}$ are chosen randomly, independently and uniformly in $\mathbb{F}_q$. Then $M$ is invertible with probability $\prod_{i=1}^{n}(1-q^{-i})$. This probability is greater than the limit $c(q) = \prod_{i=1}^{\infty}(1-q^{-i})$.*

*When $q$ is large, $c(q)$ is very close to $1 - 1/q$ and has the explicit lower bound $c(q) \geq \left(\frac{q-1}{q}\right)^{\frac{q}{q-1}}$.*

Since a system behaves generically if and only if all the matrices $B$ are invertible, we obtain the probability that our F4 variant works successfully:

**Theorem 4** *The algorithm* `F4Remake` *outputs a Gröbner basis of a random system $f_1, \ldots, f_r \in \mathbb{F}_q[\underline{X}]$ with a probability that is heuristically greater than $c(q)^{n_{step}}$, assuming that the precomputation has been done with* `F4Precomp` *in $n_{step}$ steps, for a system $f_1^0, \ldots, f_r^0 \in \mathbb{F}_q[\underline{X}]$ that behaves generically.*

For a system of generic polynomials, it is known that the number of steps $n_{step}$ during the execution of F4 (for a degree-graded monomial order) is at most equal to the degree of regularity $d_{reg}$ of the homogenized system, which is smaller than the Macaulay bound $\sum_{i=1}^{r}(\deg F_i - 1) + 1$ [23]; this bound is sharp when the system is underdetermined. Since $c(q)$ converges to 1 when $q$ goes to infinity, for a fixed degree of regularity the probability of success of our algorithm will be very close to 1 when the base field $\mathbb{F}_q$ is sufficiently large.

In practice, it is rather uncommon to deal with completely random polynomials. For many applications, the involved polynomial systems actually depend of a small number of random parameters, hence a more general framework would be the following:

**Definition 5** *Let $F_1, \ldots, F_r$ be polynomials in $\mathbb{K}[Y_1, \ldots, Y_\ell][\underline{X}]$. We call the image of the map*

$$\mathbb{K}^\ell \to \mathbb{K}[\underline{X}]^r, \quad y = (y_1, \ldots, y_\ell) \mapsto (F_1(y), \ldots, F_r(y))$$

*a parametrized family (or family for short) of systems. We call the system $(F_1, \ldots, F_r)$ the generic parametrized system of the family.*

A system of generic polynomials is of course a special case of a generic parametrized system. As above, the `F4Remake` algorithm will give correct results for systems $f_1, \ldots, f_r$ in a family that behave like its associated generic parametrized system. The probability that this happens is difficult to estimate since it obviously depends of the family considered, but is usually better than for systems of generic polynomials. An important class of examples is when the highest degree homogeneous part of the $F_i$ has coefficients in $\mathbb{K}$ (instead of $\mathbb{K}[Y_1, \ldots, Y_\ell]$). Then all systems of this parametrized family behave generically until the first fall of degree occurs. As a consequence, the probability of success of our algorithm can be quite good even when the base field is relatively small, see section 4.2 for an example.

### 3.2 Change of characteristic

Another application of our algorithm is the computation of Gröbner bases of "random" polynomial systems over a large field, using a precomputation done over a small finite field. Even for a single system $f_1, \ldots, f_r$ in $\mathbb{F}_p[\underline{X}]$, it is sometimes more advantageous to precompute the Gröbner basis of a system $f_1', \ldots, f_r'$ with $\deg f_i = \deg f_i'$ in $\mathbb{F}_{p'}[\underline{X}]$ for a small prime $p'$, and then use `F4Remake` on the initial system, than to directly compute the Gröbner basis with F4. The estimated probabilities derived in section 3.1 do not directly apply to this situation, but a similar analysis can be done.

We recall that for every prime number $p$, there exists a well-defined reduction map $\mathbb{Q}[\underline{X}] \to \mathbb{F}_p[\underline{X}]$, which sends a polynomial $P$ to $\bar{P} = cP \mod p$, where $c \in \mathbb{Q}$ is such that $cP$ belongs to $\mathbb{Z}[\underline{X}]$ and is primitive (i.e. the gcd of its coefficients is one). Let $I = \langle f_1, \ldots, f_r \rangle$ be an ideal of $\mathbb{Q}[\underline{X}]$, and let $\bar{I} = \langle \bar{f}_1, \ldots, \bar{f}_r \rangle$ be the corresponding ideal in $\mathbb{F}_p[\underline{X}]$; we note $\{g_1, \ldots, g_s\}$ the minimal reduced Gröbner basis of $I$. According to [11], we say that $p$ is a "lucky" prime if $\{\bar{g}_1, \ldots, \bar{g}_s\}$ is the minimal reduced Gröbner basis of $\bar{I}$, and "unlucky" otherwise. There is a weaker, more useful notion (adapted from [26]) of "F4 unlucky prime" or "weak unlucky prime": a prime number $p$ is called so if the computation of the Gröbner bases of $I$ and

$\bar{I}$ with F4 differs. By doing the same analysis as in section 3.1, we can show that $p$ is weakly unlucky if and only if one of the above-defined matrices $B$ is not invertible. As before, these matrices can heuristically be considered as random and thus we obtain that the probability that a prime $p$ is not weakly unlucky, is bounded from below by $c(p)^{n_{step}}$. So, if we want to compute the Gröbner basis of a system $f_1, \ldots, f_r \in \mathbb{F}_p[\underline{X}]$ where $p$ is a large prime, we can lift this system to $\mathbb{Q}[\underline{X}]$ and then reduce it to $f'_1, \ldots, f'_r \in \mathbb{F}_{p'}[\underline{X}]$ where $p'$ is a small prime number. Then we execute `F4Precomp` on the latter system and use the precomputation on the initial system with `F4Remake`. This will produce the correct result if $p$ and $p'$ are not weakly unlucky, thus $p'$, while small enough so that the precomputation takes the least time possible, must be large enough so that the probability $c(p')^{n_{step}}$ is sufficiently close to 1.

In practice, this last approach should be used whenever possible. If one has to compute several Gröbner bases over a large field $\mathbb{F}_q$ of systems of the same parametrized family, the precomputation should not be done over $\mathbb{F}_q$, but rather over a smaller field. We will adopt this strategy in almost all the applications presented in section 4.

### 3.3 Complexity

Generally, it is difficult to obtain good estimates for the complexity of Gröbner basis computation algorithms, especially of those based on Buchberger's approach. However, we can give a broad upper bound of the complexity of `F4Remake`, by observing that it can be reduced to the computation of the row echelon form of a $D$-Macaulay matrix of the homogenized system, whose useless rows would have been removed. In the case of generic systems, $D$ is equal to the degree of regularity $d_{reg}$ of the homogenized system, but may be greater for some very specific instances. Thus we have an upper-bound for the complexity of our algorithm:

**Proposition 6** *The number of field operations performed by* `F4Remake` *on a system of random polynomials over* $\mathbb{K}[X_1, \ldots, X_n]$ *is bounded by*

$$O\left(\binom{d_{reg}+n}{n}^{\omega}\right)$$

*where* $d_{reg}$ *is the degree of regularity of the homogenized system and* $\omega$ *is the constant of matrix multiplication.*

Since there is no reduction to zero as well with F5 (under the assumption that the system is semi-regular), the same reasoning applies and gives the same upper-bound, cf [2]. However, we emphasize that these estimates are not really sharp and do not reflect the difference in performances between the two algorithms. Indeed, `F4Remake` has two main advantages over F5: the polynomials it generates are fully reduced, and it avoids the incremental structure of F5. More precisely, the F5 criterion relies on the use of a signature or label for each polynomial, and we have already mentioned in the introduction that signature compatibility conditions prohibit some reductions; therefore, the polynomials generated by F5 are not completely reduced, or are even redundant [12]. This incurs either more costly reductions later in the algorithm or a larger number of critical pairs. Secondly, the incremental nature of F5 implies that the information provided by the last system polynomials cannot be used to speed up the first stages of the computation.

Thus, our F4 variant should be used preferentially as soon as several Gröbner bases have to be computed and the base field is large enough for this family of systems. Nevertheless, the F5 algorithm remains irreplaceable when the Gröbner basis of only one system has to be computed, when the base field is too small (in particular over $\mathbb{F}_2$) or when the systems are so large that a precomputation would not be realisable.

## 4 Applications

In all applications, the variant `F4Remake` is compared with an implementation of F4 which uses the same primitives and structures (in language C), and also with the proprietary software Magma (V2.15-15) whose

implementation is probably the best publicly available for the considered finite fields. Unless otherwise specified, all tests are performed on a 2.6 GHz Intel Core 2 Duo processor and times are given in seconds.

### 4.1 Index calculus

An index calculus method has been recently proposed in [10, 17] for the resolution of discrete logarithm on $E(\mathbb{F}_{q^n})$ where $E$ is an elliptic curve defined over a small degree extension field. In order to find "relations", they make use of Semaev's idea [27] which allows to convert the relation search into the resolution of a multivariate polynomial system. A variation of this approach is given in [19], where relations with a slightly different form are considered: it has the advantage of leading to overdetermined systems and is thus faster in practical cases. We focus on the resolution of the polynomial systems arising from this last attack in the special case of $E(\mathbb{F}_{p^5})$ where $p$ is a prime number. The polynomial systems in this example fit into the framework of parametrized families: the coefficients polynomially depend of the $x$-coordinate of a random point $R \in E(\mathbb{F}_{p^5})$ (and also of the equation of the curve $E$). Our algorithm is particularly relevant for this example because of the large number of relations to collect, leading to an average of $4!p^2$ systems to solve. Moreover, $p$ is large in all applications so the probability of success of our F4 variant is extremely good.

We cite directly the results from [19], where the `F4Remake` algorithm has first been introduced. The systems to solve are composed of 5 equations defined over $\mathbb{F}_p$ of total degree 8 in 4 variables. Degrevlex Gröbner bases of the corresponding ideals over several prime fields of size 8, 16, 25 and 32 bits are computed. The probabilities of failure are estimated under the assumption that the systems are random, and knowing that the computation takes 29 steps.

| size of $p$ | est. failure probability | F4Precomp | F4Remake | F4 | F4 Magma |
|---|---|---|---|---|---|
| 8 bits | 0.11 | 8.963 | 2.844 | 5.903 | 9.660 |
| 16 bits | $4.4 \times 10^{-4}$ | (19.07) | 3.990 | 9.758 | 9.870 |
| 25 bits | $2.4 \times 10^{-6}$ | (32.98) | 4.942 | 16.77 | 118.8 |
| 32 bits | $5.8 \times 10^{-9}$ | (44.33) | 8.444 | 24.56 | 1046 |

**Fig. 1.** Experimental results on $E(\mathbb{F}_{p^5})$

As explained in section 3.2, it is sufficient to execute the precomputation on the smaller field to get a list of polynomial multiples that works for the other cases; the timings of `F4Precomp` over the fields of size 16, 25 and 32 bits are thus just indicative. The above figures show that the precomputation overhead is largely compensated as soon as there are more than two subsequent computations. Note that it would have been hazardous to execute `F4Precomp` on a smaller field as the probability of failure increases rapidly. It is mentioned in [19] that the systems have also been solved with a personal implementation of F5, and that the size of the Gröbner basis it computes at the last step before minimalization is surprisingly large (17249 labeled polynomials against no more than 2789 polynomials for both versions of F4). As a consequence, the timings of F5 obtained for these systems are much worse than those of F4 or its variants. This shows clearly that on this example, it is much more efficient to apply our algorithm rather than F5.

### 4.2 Hybrid approach

The hybrid approach proposed in [3] relies on a trade-off between exhaustive search and Gröbner basis computation. The basic idea is that when one wants to find a solution of a given system $f_1, \ldots, f_r \in$

$\mathbb{K}[X_1, \ldots, X_n]$, it is sometimes faster to try to guess a small number of variables $X_1, \ldots, X_k$. For each possible $k$-tuple $(x_1, \ldots, x_k)$, one computes the Gröbner basis of the corresponding specialized system $f_1(x_1, \ldots, x_k), \ldots, f_r(x_1, \ldots, x_k) \in \mathbb{K}[X_{k+1}, \ldots, X_n]$ until a solution is found; the advantage is that the specialized systems are much simpler to solve than the initial one.

The hybrid approach is thus a typical case when many systems of the same shape have to be solved and fits perfectly into the framework of parametrized families we have described in section 3.1. However, this method is most useful when the search space is reasonably small, which implies in particular that the size of the base field cannot be too large, so one should be wary of the probability of success before applying our F4 variant to this context.

As an example, we consider the cryptanalysis of the Unbalanced Oil and Vinegar system (UOV, [21]), described in [3]. Briefly, the attack can be reduced to the resolution of a system of $n$ quadratic equations in $n$ variables over a finite field $\mathbb{K}$; for the recommended set of parameters, $n = 16$ and $\mathbb{K} = \mathbb{F}_{16}$. Although the base field is quite small, our F4 variant has rather good results in this cryptanalysis: this is due to the fact that the quadratic part of the evaluated polynomials $f_i(x_1, \ldots, x_k) \in \mathbb{K}[X_{k+1}, \ldots, X_n]$ does not depend of the values of the specialized variables $X_1, \ldots, X_k$, and hence all the systems behave generically until the first fall of degree. For instance, for $k = 3$ the computation with F4 takes 6 steps, and no fall of degree occurs before the penultimate step, so a heuristic estimation of the probability of success is $c(16)^2 \simeq 0.87$. To check this estimate we have performed an exhaustive exploration of the search space $\mathbb{F}_{16}^3$ using `F4Remake`. The actual probability of success is 80.859%, which is satisfying but somewhat smaller than estimated. The difference can be readily explained by the fact that the systems are not completely random.

### 4.3 MinRank

We briefly recall the MinRank problem: given $m + 1$ matrices $M_0, M_1, \ldots, M_m \in \mathcal{M}_n(\mathbb{K})$ and a positive integer $r$, is there a $m$-tuple $(\alpha_1, \ldots, \alpha_m) \in \mathbb{K}^m$ such that $\text{Rank}\left(\sum_{i=1}^{m} \alpha_i M_i - M_0\right) \leq r$.

We focus on the challenge A proposed in [8]: $\mathbb{K} = \mathbb{F}_{65521}; m = 10; n = 6; r = 3$. The Kipnis-Shamir's attack converts instances of the MinRank problem into quadratic multivariate polynomial systems [22]. For the set of parameters from challenge A, we thus have to solve systems of 18 quadratic equations in 20 variables, and since they are underdetermined, we can specialize two variables without loss of generality. These systems can be solve either directly or with the hybrid approach [16]; in the first case, our F4 variant will be relevant only if one wants to break several different instances of the MinRank problem.

Experiments with F4 and our variant show that, either for the full systems or the systems with one specialized variable, the matrices involved at different steps are quite large (up to $39138 \times 22968$) and relatively sparse (less than 5% non-zero entries). With both types of systems, a lot of reductions to zero occurs; for example, we have observed that for the full system at the 8th step, 17442 critical pairs among 17739 reduce to zero. This makes it clear that the classic F4 algorithm is not well suited for these specific systems.

It is difficult to compare our timings with those given in [16] using F5: besides the fact that the experiments were executed on different computers, the linear algebra used in Faugère's FGb implementation of F5 (whose source code is not public) seems to be highly optimized, even more so than in Magma's implementation of F4. On this point, our own implementation is clearly not competitive: for example, at the 7th step for the full system, Magma's F4 reduces a $26723 \times 20223$ matrix in 28.95 sec, whereas at the same step our implementation reduces a slightly smaller matrix of size $25918 \times 19392$ in 81.52 sec. Despite these limitations, we have obtained timings comparable with those of [16], listed in the table below. This means that with a more elaborate implementation of linear algebra, our F4 variant would probably be the most efficient for these systems.

| | F5 | F4Remake | F4 | F4 Magma |
|---|---|---|---|---|
| full system | 30.0 | 27.87 | 320.2 | 116.6 |
| 1 specialized variable | 1.85 | 2.605 | 9.654 | 3.560 |

**Fig. 2.** Experimental results on MinRank

Computations were executed on a Xeon bi-processor 3.2 GHz for F5. The results of `F4Remake` have been obtained after a precomputation over $\mathbb{F}_{257}$ of 4682 sec for the full system and 113 sec for the system with one variable specialized.

### 4.4 Katsura benchmarks

To illustrate the approach presented in section 3.2, we have applied our algorithm to the computation of the Gröbner bases of the Katsura11 and Katsura12 systems [20], over two prime fields of size 16 and 32 bits. As already explained, the idea is to run a precomputation on a small prime field before executing `F4Remake` over a large field (actually, for Katsura12 the first prime $p = 251$ we chose was weakly unlucky). The timings show that for both systems, the speed gain on 32 bits compensates the precomputation overhead, contrarily to the 16 bits case.

| | 8 bits | 16 bits | | | 32 bits | | |
|---|---|---|---|---|---|---|---|
| | Precomputation | F4Remake | F4 | F4 Magma | F4Remake | F4 | F4 Magma |
| Katsura11 | 27.83 | 9.050 | 31.83 | 19.00 | 15.50 | 60.93 | 84.1 |
| Katsura12 | 202.5 | 52.66 | 215.4 | 143.3 | 111.4 | 578.8 | $> 5\,h$ |

**Fig. 3.** Experimental results on Katsura11 and Katsura12

As a side note, we observed that surprisingly, the matrices created by F4 are quite smaller in our version than in Magma (e.g. $15393 \times 19368$ versus $20162 \times 24137$ at step 12 of Katsura12); of course, both version still find the same new polynomials at each step. This phenomenon was already present in the previous systems, but not in such a proportion. This seems to indicate that our implementation of the `Simplify` subroutine is much more efficient.

## 5 Conclusion

We have presented in this article a variant of the F4 algorithm that provides a new and very efficient probabilistic method for computing Gröbner bases; it is especially designed for the case where many similar polynomial systems have to be solved. We have given a precise analysis of this context, estimated the probability of success, and evaluated both theoretically and experimentally the performances of our algorithm, showing that it is well adapted for algebraic attacks on cryptosystems.

Since Faugère's F5 algorithm is considered as the most efficient tool for computing Gröbner bases, we have tried as much as possible to compare its performances with our F4 variant. Clearly, F5 remains irreplaceable when the Gröbner basis of only one system has to be computed or when the base field is too small, in particular over $\mathbb{F}_2$. However, our method should be used preferentially as soon as several Gröbner bases have to be computed and the base field is large enough for the considered family of systems. The obtained timings support in part this claim, indicating that with a more elaborate implementation of linear algebra our algorithm would outperform F5 in most cases.

## References


1. G. Bard. *Algebraic Cryptanalysis*. Springer-Verlag, New York, first edition, 2009.
2. M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. Presented at MEGA'05, Eighth International Symposium on Effective Methods in Algebraic Geometry, 2005.
3. L. Bettale, J.-C. Faugère, and L. Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, pages 177–197, 2009.
4. W. Bosma, J. J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comput.*, 24(3/4):235–265, 1997.
5. B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, Austria, 1965.
6. B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In E. W. Ng, editor, *Proc. of the EUROSAM 79*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21. Copyright: Springer, Berlin - Heidelberg - New York, 1979.
7. B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N. Bose, editor, *Multidimensional systems theory, Progress, directions and open problems, Math. Appl. 16*, pages 184–232. D. Reidel Publ. Co., 1985.
8. N. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In *Advances in Cryptology – ASIACRYPT 2001*, pages 402–421. Springer, 2001.
9. N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Advances in Cryptology – EUROCRYPT 2000*, pages 392–407. Springer, 2000.
10. C. Diem. On the discrete logarithm problem in elliptic curves. Preprint, available at: `http://www.math.uni-leipzig.de/~diem/preprints/dlp-ell-curves.pdf`, 2009.
11. G. L. Ebert. Some comments on the modular approach to Gröbner-bases. *SIGSAM Bull.*, 17(2):28–32, 1983.
12. C. Eder and J. Perry. F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases. arXiv/0906.2967, 2009.
13. J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, June 1999.
14. J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of ISSAC 2002*, New York, 2002. ACM.
15. J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *CRYPTO*, pages 44–60, 2003.
16. J.-C. Faugère, F. Levy-Dit-Vehel, and L. Perret. Cryptanalysis of MinRank. In *Advances in Cryptology – CRYPTO 2008*, pages 280–296, Berlin, Heidelberg, 2008. Springer-Verlag.
17. P. Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *J. Symbolic Computation*, 2008. doi:10.1016/j.jsc.2008.08.005.
18. R. Gebauer and H. M. Möller. On an installation of Buchberger's algorithm. *J. Symbolic Comput.*, 6(2-3):275–286, 1988.
19. A. Joux and V. 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, 2010.
20. S. Katsura, W. Fukuda, S. Inawashiro, N. M. Fujiki, and R. Gebauer. Distribution of effective field in the Ising spin glass of the $\pm J$ model at $T = 0$. *Cell Biochem. Biophys.*, 11(1):309–319, 1987.
21. A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar signature schemes. In *Advances in Cryptology – EUROCRYPT'99*, pages 206–222. Springer, 1999.
22. A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in Cryptology – CRYPTO' 99*, pages 19–30. Springer Berlin, Heidelberg, 1999.
23. D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 146–156. Springer, Berlin, 1983.
24. F. Macaulay. Some formulae in elimination. *Proceedings of London Mathematical Society*, pages 3–38, 1902.
25. M. S. E. Mohamed, W. S. A. E. Mohamed, J. Ding, and J. Buchmann. MXL2: Solving polynomial equations over $GF(2)$ using an improved mutant strategy. In *PQCrypto*, pages 203–215. Springer, 2008.
26. T. Sasaki and T. Takeshima. A modular method for Gröbner-basis construction over $\mathbb{Q}$ and solving system of algebraic equations. *J. Inf. Process.*, 12(4):371–379, 1989.
27. I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Cryptology ePrint Archive, Report 2004/031, 2004.