Algebraic Attacks on Block Ciphers from a Gröbner Basis Perspective

It's like Gaussian elimination, but exponential

Martin Albrecht (malb@informatik.uni-bremen.de)

"Thus, if we could show that solving a certain system requires at least as much work as solving a system of simultaneous equations in a large number of unknowns, of a complex type, then we would have a lower bound of sorts for the work characteristic." [Sha49]

Outline

Some notation and definitions

- $P = k[x_0, \ldots, x_{n-1}]$; k a field
- I is an ideal $\subset P$. $m, n \in I \rightarrow m + n \in I; v \in P \rightarrow v \cdot m \in I$
- $< f_0, \ldots, f_{n-1} >$ is the ideal spanned by $f_0, \ldots, f_{n-1}$.
- $V(f_0, \ldots, f_{n-1}) = \{(a_0, \ldots, a_{m-1}) \in k^m : f_i(a_0, \ldots, a_{m-1}) = 0$ for all $0 \leq i < n\}$.
- $V(I)$ is the variety of I. Especially, if $I =< f_0, \ldots, f_{n-1} >$, then $V(I) = V(f_0, \ldots, f_{n-1})$

The Task

Given a set "complicated" set $f_0, \ldots, f_{n-1}$, compute a simpler set $g_0, \ldots, g_{m-1}$, such that $< f_0, \ldots, f_{n-1} >=< g_0, \ldots, g_{m-1} >$ and consequently $V(f_0, \ldots, f_{n-1}) = V(g_0, \ldots, g_{m-1})$.

Those "complicated" sets are for example:

AES (128-bit, 10 rounds) 8000 equations in 1600 variables over $\mathbb{F}_2$ [CP02] or 5248 equations in 3968 variables over $\mathbb{F}_{2^8}$ [MR02].

CTC (255-bit, 6 rounds) 11985 equations in 6375 variables over $\mathbb{F}_2$.

How do we know where to look for a simpler set?

Little Detour: Monomial Orderings

Monomials can be ordered in different ways, i.e. there is no canonical ordering.
Important examples include:

lexicographical Given e.g. a, b, c then a is always greater than b . . . like in a phone book.

degree **lex**icographical Sort by degrees first, then use *lex*

block Every element from one block B_1 is always bigger than any element from another block B_2 (like *lex*), but inside the blocks use e.g. *deglex*.

Leading monomials etc. are always considered with respect to some monomial ordering.

(Reduced) Gröbner Bases

Definition (Gröbner Basis)

Fix a monomial order. A finite subset $G = \{g_0, \ldots, g_{m-1}\}$ of an ideal I is said to be a *Gröbner basis* or standard basis if

$$\langle LT(g_0), \ldots, LT(g_{m-1})\rangle = \langle LT(I)\rangle.$$

Definition (Reduced Gröbner Basis)

A *reduced Gröbner basis* for a polynomial ideal I is a Gröbner basis for G such that:

1. $LC(f) = 1$ for all $f \in G$;
2. For all $f \in G$, no monomial of f lies in $\langle LT(G - \{f\})\rangle$.

Example

Consider (and ignore abuse of notation):

$$0 = K_{0,0} + K_{1,2},\ 0 = K_{0,2} + K_{1,1},\ 0 = K_{0,1} + K_{1,0},\ 0 = 1 + K_{1,2} + Z_{1,2},\ 0 = K_{1,1} + Z_{1,1},\ 0 = K_{1,0} + Z_{1,0},$$

$$0 = Z_{1,1} + Y_{1,2} + Y_{1,1},\ 0 = Z_{12} + Y_{10},\ 0 = Z_{10} + Y_{11} + Y_{10},\ 0 = K_{02} + X_{12},\ 0 = 1 + K_{01} + X_{11},$$

$$0 = K_{00} + X_{10},\ 0 = Y_{12} + Y_{10}Y_{11} + X_{10},\ 0 = Y_{12} + Y_{11} + Y_{11}Y_{12} + Y_{10} + X_{12} + X_{10},$$

$$0 = Y_{12} + Y_{10} + X_{12} + X_{12}Y_{11} + X_{10},\ 0 = 1 + Y_{12} + Y_{11} + Y_{10}Y_{12} + X_{11} + X_{10},$$

$$0 = 1 + Y_{12} + Y_{11} + Y_{10} + X_{11} + X_{11}Y_{10} + X_{10},\ 0 = 1 + Y_{12} + Y_{11} + Y_{10} + X_{11} + X_{11}X_{12} + X_{10},$$

$$Y_{12} + Y_{10} + X_{12}Y_{10} + X_{10}Y_{12},\ 0 = 1 + Y_{10} + X_{12} + X_{11} + X_{11}Y_{12} + X_{10}Y_{12},$$

$$0 = 1 + Y_{11} + X_{12}Y_{12} + X_{11} + X_{10} + X_{10}Y_{12},\ X_{11}Y_{11} + X_{10} + X_{10}Y_{12},\ Y_{11} + Y_{10} + X_{12} + X_{10}Y_{11},$$

$$0 = 1 + Y_{11} + X_{11} + X_{10}Y_{10},\ 0 = 1 + Y_{11} + X_{11} + X_{10}X_{12},\ 0 = 1 + Y_{10} + X_{12} + X_{11} + X_{10} + X_{10}X_{11}$$

The reduced Gröbner basis with respect to the lex monomial ordering is:

$$0 = K_{02}, 0 = 1 + K_{01}, 0 = 1 + K_{00}, 0 = 1 + K_{12}, 0 = K_{11}, 0 = 1 + K_{10}, 0 = Z_{12}, 0 = Z_{11}, 0 = 1 + Z_{10}, 0 =$$

$$1 + Y_{12}, 0 = 1 + Y_{11}, 0 = Y_{10}, 0 = X_{12}, 0 = X_{11}, 0 = 1 + X_{10}$$

More Notation

To State the General Theorem:

- An ideal is zero-dimensional if $V(I)$ is finite.
- The radical of I denoted by $\sqrt{I}$, is the set $\{f : f^e \in I \text{ for some integer } e \geq 1\}$.
- A perfect field is a field of chracteristic p where every element has a $p - th$ root or the characteristic is zero.
- An elimination ideal is defined as: Given $I = \langle f_0, \ldots, f_{m-1} \rangle \subset k[x_0, \ldots, x_{n-1}]$, the l-th elimination ideal I_l is the ideal of $k[x_{l+1}, \ldots, x_{n-1}]$ defined by $I_l = I \cap k[x_{l+1}, \ldots, x_{n-1}]$.

The Shape Lemma I

Theorem (The Shape Lemma)

Let k be a perfect field, let $I \subset P$ be a zero-dimensional radical ideal. Let $g_{n-1} \in k[x_{n-1}]$ be the monic generator of the elimination ideal $I \cap k[x_{n-1}]$, and let $d = deg(g_{n-1})$. Then the following statements are true:

1. *The reduced Gröbner basis of the ideal I with respect to the lexicographic ordering $x_0 > \cdots > x_{n-1}$ is of the form*

$$\{x_0 - g_0, \ldots, x_{n-2} - g_{n-2}, g_{n-1}\},$$

   where $g_0, \ldots, g_{n-2} \in k[x_{n-1}]$;

2. *The polynomial g_{n-1} has d distinct zeros $a_0, \ldots, a_{d-1} \in k$, and the set of zeros of I is $\{(g_0(a_i), \ldots, g_{n-2}(a_i), a_i) : i = 0, \ldots, d-1\}$.*

The Shape Lemma II

To bring an ideal over $\mathbb{F}_p$ in the form such that the shape lemma applies, add the "field polynomials" ($\{x_i^p - x_i\}$ for every $0 \leq i < n$) to the ideal. This makes sure, that:

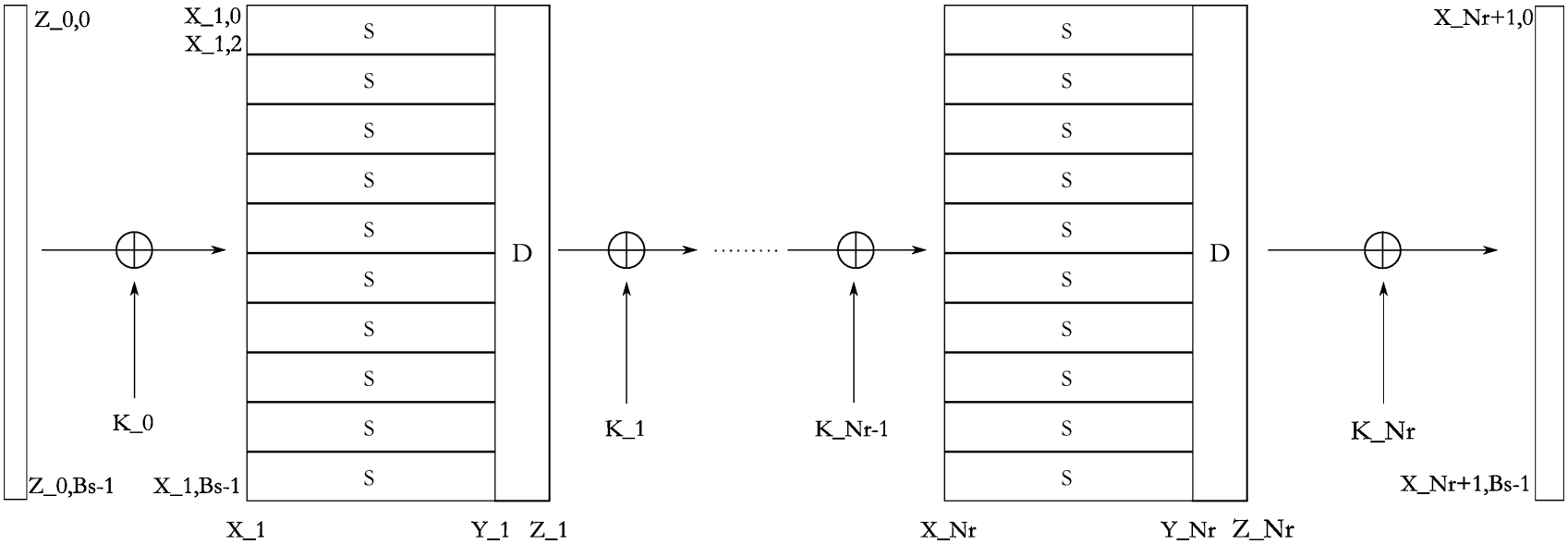
- solutions from the algebraic closue are excluded as $x_i^p - x_i$ factors completely over $\mathbb{F}_p$,
- the ideal is zero-dimensional (implied by above statement),
- the ideal is a radical ideal as $\mathrm{GCD}(\frac{d(x_i^p - x_i)}{dx_i}, x_i^p - x_i) = 1$ (Seidenberg's Lemma).

Outline

CTC Overview: Bird's Eye View I

The cipher operates on block sizes which are multiples of 3. So the block size is $B \cdot s$ where $s = 3$ and B may be chosen. The cipher is defined in rounds where each round performs the same operation on the input data except that a different round key is added each time. The output of round $i - 1$ is the input of round i. Each round consists of a parallell application of B S-boxes, the application of the linear diffusion layer, and a final key addition of the round key.

CTC Overview: Bird's Eye View II



CTC Overview: Some Details

- The S-Box is defined over $GF(2^3)$ as the non-linear random permutation $[7, 6, 0, 4, 2, 5, 1, 3]$. The transformation from $GF(2)^3$ to $GF(2^3)$ is the "natural"-mapping.
- This gives rise to 14 lineary independent quadratic equations in the input and output variables
- The diffusion layer is very thin:

$$Z_{i,(257\%Bs)} = Y_{i,0} \text{ for all } i = 1 \ldots N_r,$$
$$Z_{i,(j\cdot 1987+257\%Bs)} = Y_{i,j} + Y_{i,(j+137\%Bs)} \text{ for } j \neq 0 \text{ and all } i.$$

- The key schedule is a simple permutation of wires.

V(I)

$$P_0 + K_{0,0} + X_{1,0},$$
$$P_1 + K_{0,1} + X_{1,1},$$
$$P_2 + K_{0,2} + X_{1,2},$$

$$1 + X_{1,0} + X_{1,1} + X_{1,1}X_{1,0} + X_{1,2} + Y_{1,0},$$
$$1 + X_{1,1} + X_{1,2}X_{1,0} + Y_{1,1},$$
$$1 + X_{1,1} + Y_{1,0}X_{1,0} + Y_{1,1},$$
$$X_{1,2} + Y_{1,0} + Y_{1,1} + Y_{1,1}X_{1,0},$$
$$1 + X_{1,0} + X_{1,1} + X_{1,2}X_{1,1} + Y_{1,0} + Y_{1,1} + Y_{1,2},$$
$$1 + X_{1,0} + X_{1,1} + Y_{1,0} + Y_{1,0}X_{1,1} + Y_{1,1} + Y_{1,2},$$
$$X_{1,0} + Y_{1,1}X_{1,1} + Y_{1,2}X_{1,0},$$
$$1 + X_{1,1} + X_{1,2} + Y_{1,0} + Y_{1,2}X_{1,0} + Y_{1,2}X_{1,1},$$
$$Y_{1,0} + Y_{1,0}X_{1,2} + Y_{1,2} + Y_{1,2}X_{1,0},$$
$$X_{1,0} + X_{1,2} + Y_{1,0} + Y_{1,1}X_{1,2} + Y_{1,2},$$
$$1 + X_{1,0} + X_{1,1} + Y_{1,1} + Y_{1,2}X_{1,0} + Y_{1,2}X_{1,2},$$
$$X_{1,0} + Y_{1,1}Y_{1,0} + Y_{1,2},$$
$$1 + X_{1,0} + X_{1,1} + Y_{1,1} + Y_{1,2} + Y_{1,2}Y_{1,0},$$
$$X_{1,0} + X_{1,2} + Y_{1,0} + Y_{1,1} + Y_{1,2} + Y_{1,2}Y_{1,1},$$

$$Y_{1,0} + Y_{1,1} + Z_{1,0},$$
$$Y_{1,1} + Y_{1,2} + Z_{1,1},$$
$$Y_{1,0} + Z_{1,2},$$

$$K_{0,1} + K_{1,0},$$
$$K_{0,2} + K_{1,1},$$
$$K_{0,0} + K_{1,2},$$

$$Z_{1,0} + K_{1,0} + C_0,$$
$$Z_{1,1} + K_{1,1} + C_1,$$
$$Z_{1,2} + K_{1,2} + C_2,$$

Outline

Gröbner basis Construction

Recall the definition of a Gröbner basis. It is a set G of polynomials $g_0, \ldots g_{m-1}$ such that:

$$\langle LT(g_0), \ldots, LT(g_{m-1}) \rangle = \langle LT(I) \rangle.$$

Now, try to create elements in $\langle LT(I) \rangle$ and not in $\langle LT(g_0), \ldots, LT(g_{m-1}) \rangle$. If you **find** such an element **add it** to the basis. If such an element provably cannot be constructed G is a Gröbner basis. This procedure **terminates** as the ideals of leading terms created this way are strictly increasing and such a sequence **must stabilize** eventually due to the **Ascending Chain Condition**. At this point $\langle LT(g_0), \ldots, LT(g_{m-1}) \rangle = \langle LT(I) \rangle$.

S-Polynomials

Bruno Buchberger showed that every cancelation of leading terms may be accounted to *S-polynomials*.

Definition (S-Polynomial)

Let $f, g \in k[x_1, \ldots, x_n]$ be polynomials $\neq 0$ and define $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$. Then the S-polynomial of f and g is defined as

$$S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

Polynomial Reduction

The S-polynomial h of g_i, g_j is not in $< \mathrm{LT}(g_i), \mathrm{LT}(g_j) >$ but it is in $< \mathrm{LT}(I) >$. It may be in $G_r =< \{g_k | k \neq i, j\} >$.

Definition

Let $G = \{g_0, \ldots, g_{m-1}\} \subset P$. Given a polynomial $h \in P$, we say that h reduces to zero modulo G, written

$$h \xrightarrow[G]{} 0,$$

if h can be written in the form

$$h = a_0 g_0 + \cdots + a_{m-1} g_{m-1},$$

such that whenever $a_i g_i \neq 0$, we have $h \geq a_i g_i$.

Buchberger's Algorithm

```
def buchberger(F):
 """
 INPUT:
     F -- a finite subset of P[x]

 OUTPUT:
     A Groebner basis for the ideal <F>.
 """
 G = F
 G2 = set()
 while G2!=G
   G2 = G
   for p in G2:
     for q in G2:
       if p!=q:
         S = "S-pol(p,q) reduced modulo G2"
         if S != 0:
           G.add(S)
 return G
```

Runtime I

- Intermediate basis grows pretty quickly
- Major bottleneck is reduction modulo G2
- Need strategy which S-polynomial to construct in which order
- Need criteria which S-polynomial reduces to zero
- Computing with respect to *lex* takes much longer than e.g. *deglex*
- Runtime is exponential or worse in general. Solving polynomial equation systems in NP-hard.
- We don't know much about the actual runtime Buchberger's algorithm applied to a given ideal basis.

Runtime II

Situation could be better for algebraic attacks:

- zero-dimensional (one solution)
- systems are often sparse yet overdefined
- working over simple fields like $\mathbb{F}_2$
- systems are highly structured

Several improvements and specializations to Buchberger's algorithm exist

- Gebauer-Möller installation
- F_4 and F_5
- SlimGB
- Gröbner Proofing

State of the Art: F_4 [Fau99]

Theorem

Construct the coefficient matrix A for an ideal basis F and call the (reduced) row echelon form $\tilde{A}$. Then $\tilde{F}$ constructed from $\tilde{A}$ is called the row echelon form of F. Let $\tilde{F}^+$ denote the set

$$\{g \in \tilde{F} : LM(g) \notin LM(F)\}.$$

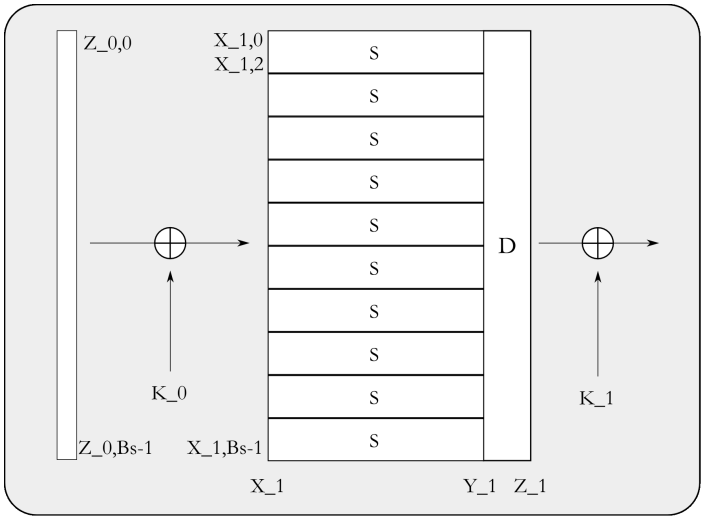
The elements of $\tilde{F}^+$ are joined with a subset H of the original F, such that:

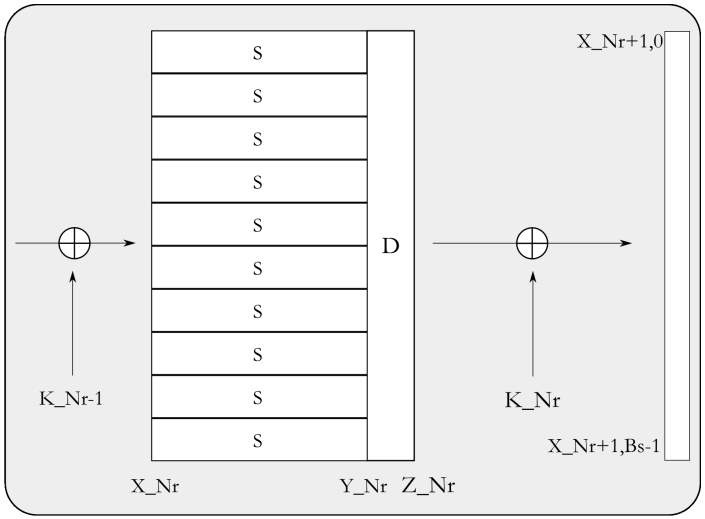
$$LM(H) = LM(F) \ and \ |H| = |LM(F)|$$

holds. Then the ideal $< F >$ is spanned by $H \cup \tilde{F}^+$.

Outline

Meet-in-the-Middle [CMR05]





Left ⟶ GB ⟵ Right

Meet-in-the-Middle Results

- Implemented on top of Singular's Gröbner basis engine
- Faster for *lex* monomial ordering than naïve approach
- Faster for *degrevlex* monomial ordering up to $B = 2$.

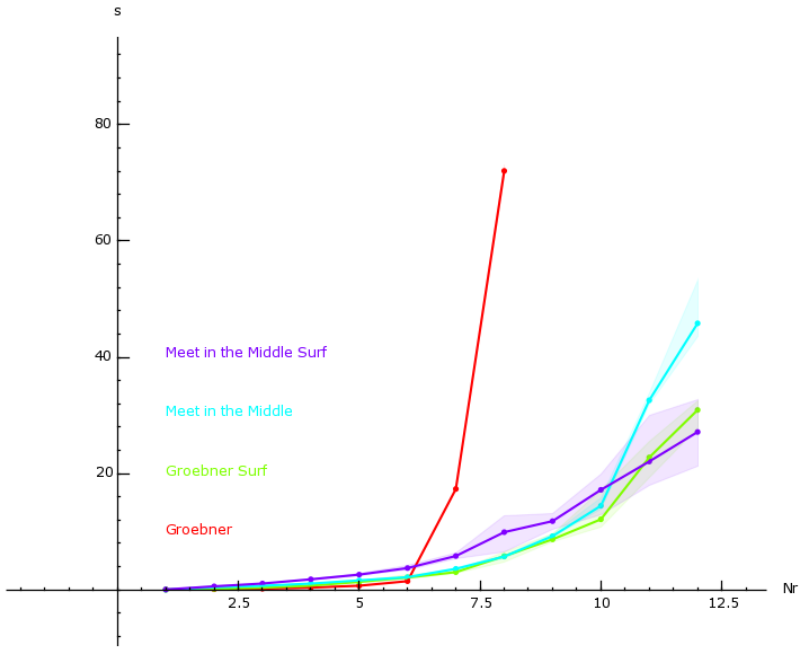
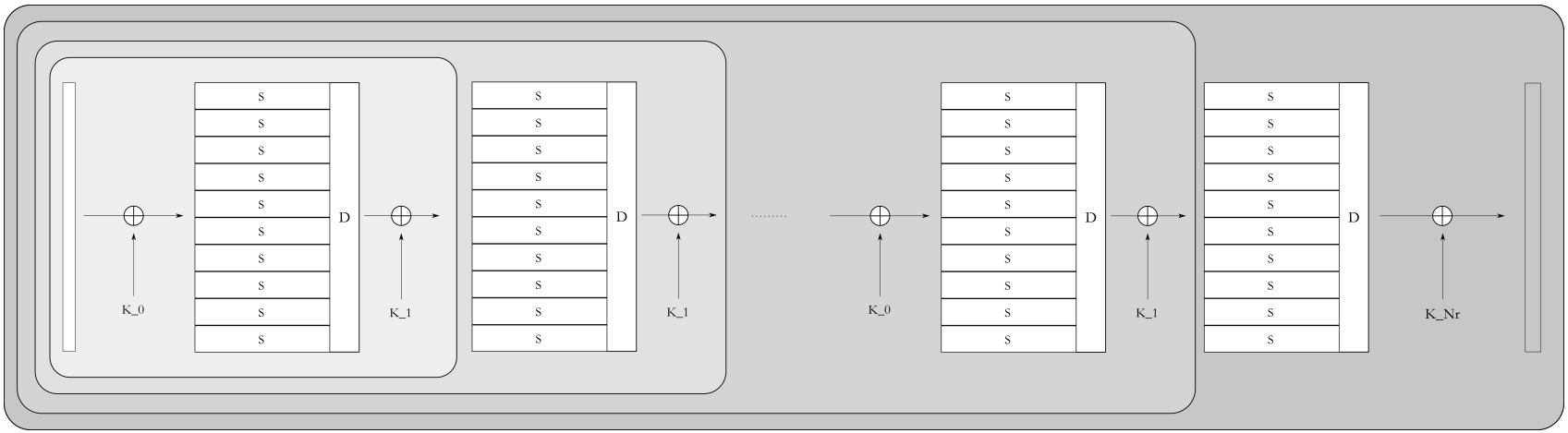


Abbildung: Runtimes for B=1 and term ordering *lex*

Gröbner Surfing: Idea



Gröbner Surfing: Algorithm

```
def groebner_surf(F):
    """
    Returns a Groebner basis for a given MQ problem F.

    INPUT:
        F -- MQ problem, separable in rounds

    OUTPUT:
        a Groebner basis for F with respect to F.ring().term_order()
    """
    singular.option("redSB")
    P = F.ring()
    gb = P.ideal([0])

    for i in range(len(F.round)):
        gb = (gb + P.ideal(F.round[i])).groebner_basis()

    return gb
```

Gröbner Surfing: Correctness

Correctness Algorithm is in fact selection strategy. It doesn't affect correctness.

Termination Buchberger's Algorithm terminates, thus Nr times Buchberger's Algorithm terminate as well.

Gröbner Surfing Results I

- Lexicographical Term Ordering
  - Faster than naïve approach and Meet-in-the-Middle for $B = 1$
- Graded Reverse Lexicographical & Block Term Ordering
  - Split equation systems in blocks by rounds, use *degrevlex* in blocks [Wei06]
  - Faster than naïve Buchberger for *degrevlex*.
  - Also: Gröbner basis looks better, as blocks eliminate.
- Why is this faster?
  - Exploits structure: We know the dependencies
  - Reduces intermediate basis grow: reduction after every round
  - Thus it is not faster for *degrevlex* in general

Gröbner Surfing Results II

A good monomial order:

```
sage: F,s = ctc_MQ(Nr=3,variable_order=1,term_order=block_order(Nr=3))
sage: F.ring()._singular_()
//    characteristic : 2
//    number of vars : 39
//         block   1 : ordering dp
//                   : names    K_3,2 K_3,1 K_3,0 Z_3,2 Z_3,1 Z_3,0
//                              Y_3,2 Y_3,1 Y_3,0 X_3,2 X_3,1 X_3,0
//                              K_2,2 K_2,1 K_2,0
//         block   2 : ordering dp
//                   : names    Z_2,2 Z_2,1 Z_2,0 Y_2,2 Y_2,1 Y_2,0
//                              X_2,2 X_2,1 X_2,0 K_1,2 Kv1,1 K_1,0
//         block   3 : ordering dp
//                   : names    Z_1,2 Z_1,1 Z_1,0 Y_1,2 Y_1,1 Y_1,0
//                              X_1,2 X_1,1 X_1,0 K_0,2 K_0,1 K_0,0
//         block   4 : ordering C
```

Gröbner Surfing Results III

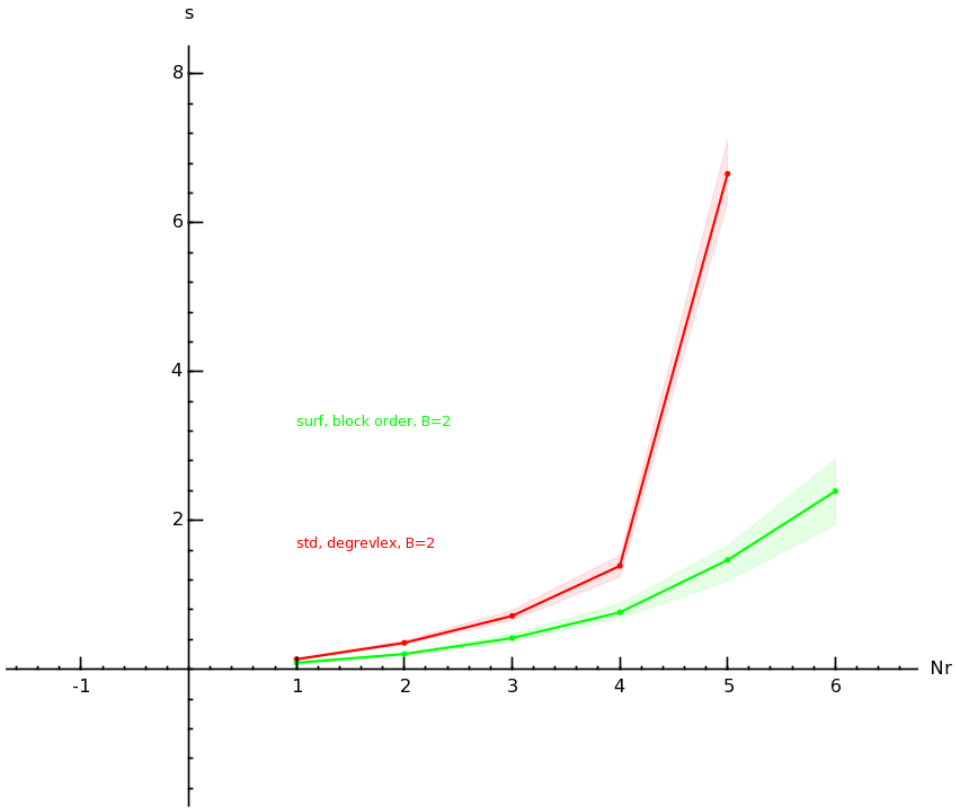


Abbildung: Runtimes for $B = 2$

Gröbner Surfing Results IV

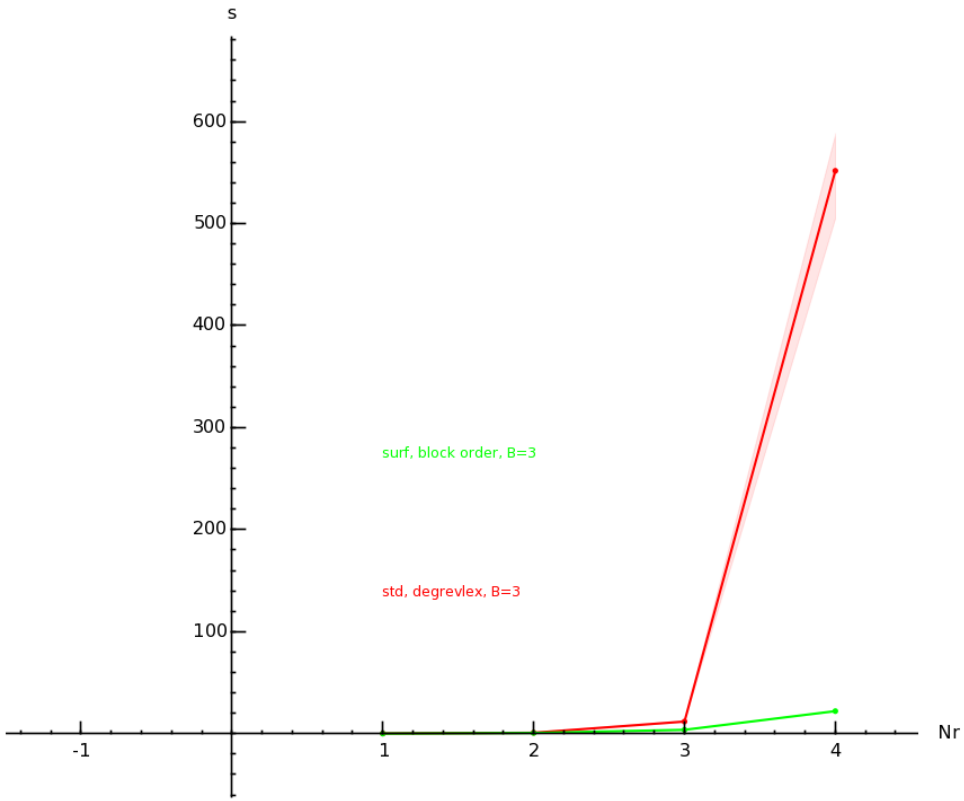


Abbildung: Runtimes for $B = 3$

Gröbner Basis without Reduction [BPW05]

- First Buchberger Criterion: *Suppose that we have $f, g \in G$, such that the leading monomials of f and g are pairwise prime. Then the S-polynomial of f and g reduces to zero.*
- We have n equations in n variables, so make sure each leading monomial is univariate and distinct from each other.
- We get a zero-dimensional Gröbner basis *CTCgb* for CTC ideals.
- Basis is still quadratic, but unclear how to exploit the fact that it is Gröbner basis; FGLM [FGLM93] and Gröbner Walk [CKM97] are too slow.

Questions?

Thank You!

References I

Johannes Buchmann, Andrei Pychkine, and Ralf-Philipp Weinmann.

Block ciphers sensitive to gröbner basis attacks.
Cryptology ePrint Archive, Report 2005/200, 2005.
available at: http://eprint.iacr.org/2005/200.

S. Collart, M. Kalkbrener, and D. Mall.

Converting bases with the gröbner walk.
In *Journal Of Symbolic Computation 24*, pages 465–469. Academic Press, 1997.

Carlos Cid, S. Murphy, and M. Robshaw.

Small scale variants of the aes.
In *Proceedings Of Fast Software Encryption 2005, LNCS 3557*, pages 145–162. Springer, 2005.
available at http://www.isg.rhul.ac.uk/~sean/smallAES-fse05.pdf.

Nicolas Courtois and Josef Pieprzyk.

Cryptanalysis of block ciphers with overdefined systems of equations.
Cryptology ePrint Archive, Report 2002/044, 2002.
available at http://eprint.iacr.org/2002/044.

Jean-Charles Faugère.

A new efficient algorithm for computing gröbner basis (f4), 1999.
available at http://modular.ucsd.edu/129-05/refs/faugere_f4.pdf.

Jean-Charles Faugère, P. Gianno, P. Lazard, and T. Mora.

Efficient computation of zero-dimensional gröbner bases by change of ordering.
In *Journal Of Symbolic Computation 16*, pages 329–344. Academic Press, 1993.

References II

S. Murphy and M. Robshaw.

Essential algebraic structure within the aes.
In *Proceedings Of Crypto 2002, LNCS 2442*, pages 1–16. Springer, 2002.
available at `http://www.isg.rhul.ac.uk/~mrobshaw/rijndael/aes-crypto.pdf`.

C. E. Shannon.

Communication theory of secrecy systems.
In *Bell System Technical Journal 28*, pages 656–715, 1949.

Ralf-Philipp Weinmann.

Private communication, 12 2006.