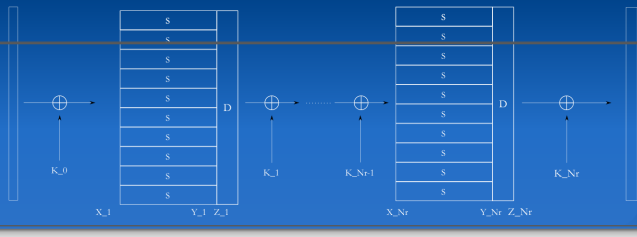
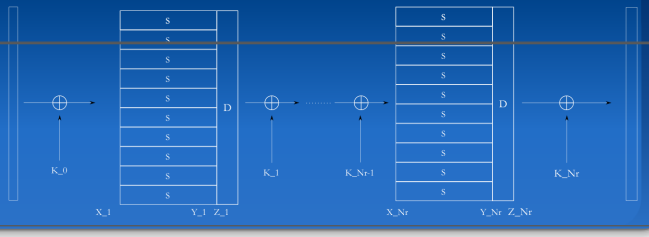


Algebraic Attacks on the Courtois Toy Cipher

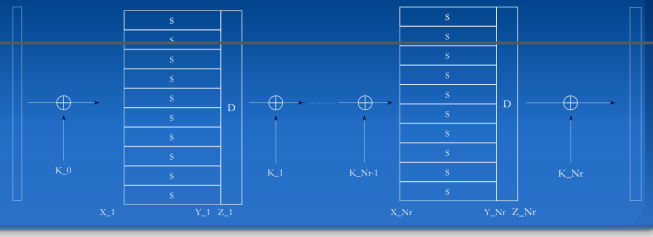
"However one should understand that the attack is quite simple and fatally will be re-discovered (and published)." [Cou06]

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

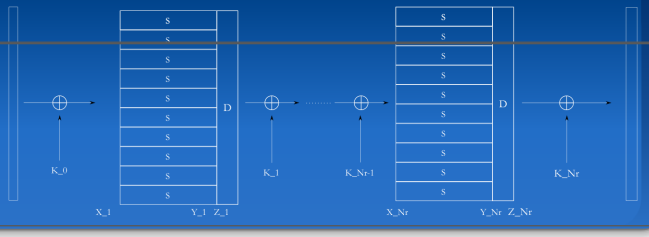
Outline



Outline

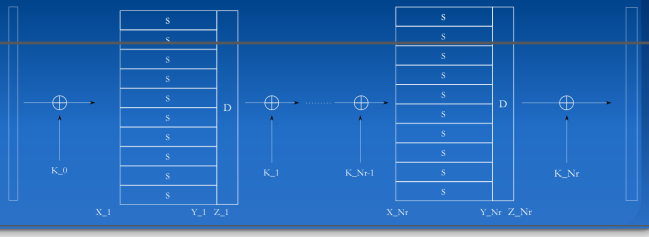


Background



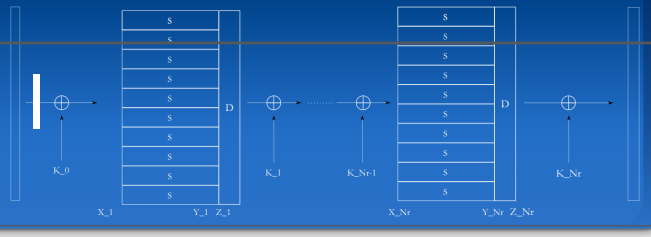
On May 13th, 2006 Nicolas Courtois published a paper [Cou06] describing yet another toy cipher to attack algebraically. He dupes this cipher Courtois Toy Cipher (CTC).
In this paper he also provides steps to produce an overdefined system of multivariate polynomial equations that – if solved – provides the key used in the encryption process. Solving this equation system to break a cipher is called algebraic attack on block ciphers in literature.
He also claims to have developed a "fast algebraic attack on block ciphers" which solves this equation system for a quite large configuration. However, this attack is unpublished.

Why CTC?



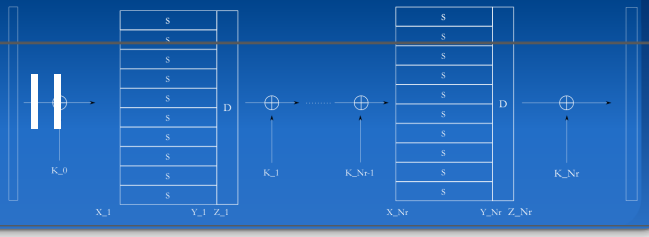
- Resist the temptation to present yet another toy cipher, use toy cipher by "big names": CTC [Cou06] or SR [CMR05].
- CTC scales up (255-bit, six rounds) and down (3-bit, one round) well
- nice properties: overdefined S-box, thin diffusion layer
- "known" to be broken using an algebraic attack
- was expected to be resistant against well-known attacks (not true anymore, see [DK06])

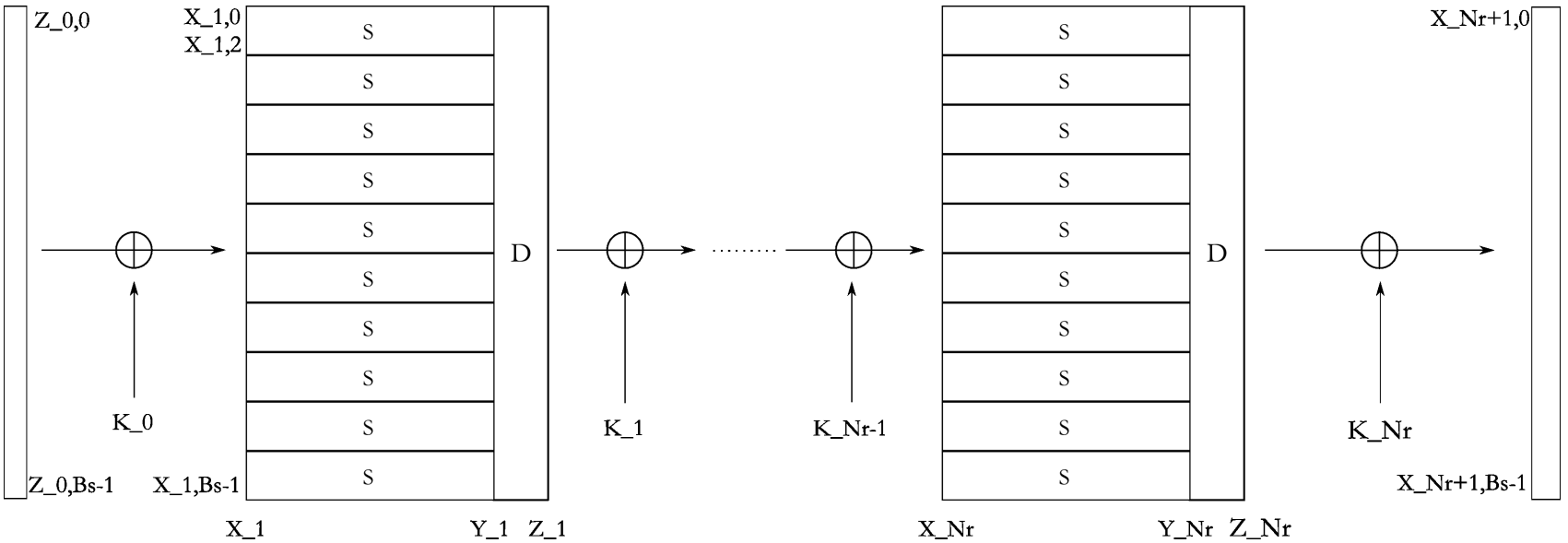
CTC Overview: Bird's Eye View I



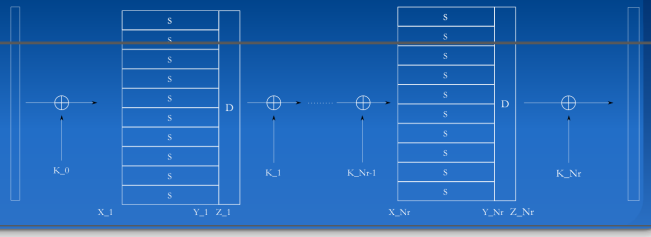
The cipher operates on block sizes which are multiples of 3. So the block size is $B \cdot s$ where $s = 3$ and B may be chosen. The cipher is defined in rounds where each round performs the same operation on the input data except that a different round key is added each time. The output of round $i-1$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

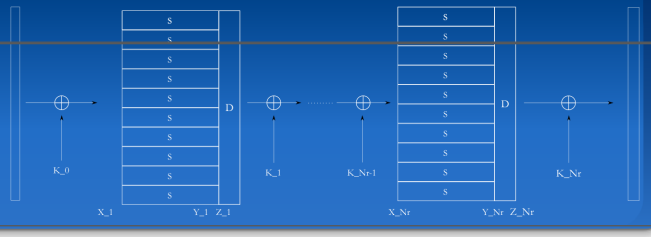


- The S-Box is defined over $GF(2^3)$ as the non-linear random permutation $[7, 6, 0, 4, 2, 5, 1, 3]$. The transformation from $GF(2)^3$ to $GF(2^3)$ is the "natural"-mapping.
- The diffusion layer is very thin:

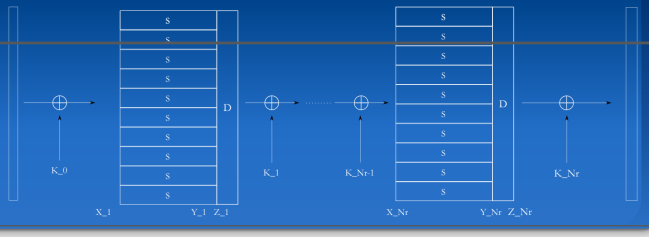
$$\begin{aligned} Z_{i,(257\%Bs)} &= Y_{i,0} \text{ for all } i = 1 \ldots N_r, \\ Z_{i,(j\cdot 1987+257\%Bs)} &= Y_{i,j} + Y_{i,(j+137\%Bs)} \text{ for } j \neq 0 \text{ and all } i. \end{aligned}$$

- The key schedule is a simple permutation of wires.

Outline



F_4 [Fau99] Idea



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

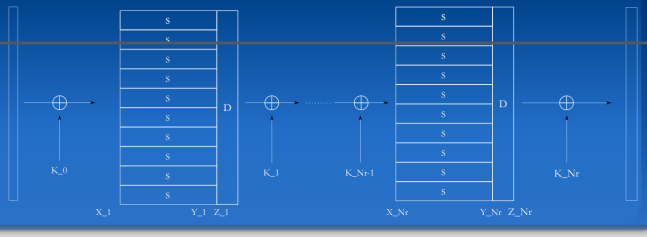
$$\{g \in \tilde{F} : LM(g) \notin LM(F)\}.$$

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

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

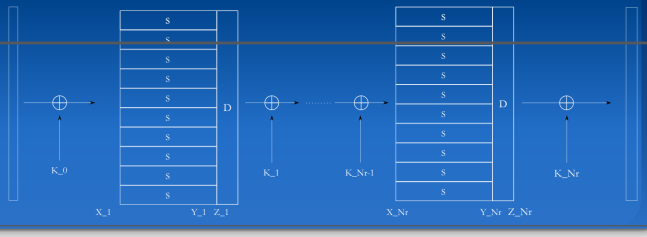
holds. Then the ideal $\langle F \rangle$ is spanned by $H \cup \tilde{F}^+$.

F_4 Results



- Thesis contains an implementation of F_4 for SAGE [SJ05].
- This implementation is slightly optimized for $\mathbb{F}_2$.
- Overall, the implementation is not very optimized but easy to read.
- Implementation seems to beat Singular's Buchberger implementation [GPS05] for *lex* in the *Quotient Ring* modulo the field ideal. $CTC_{3,3,3}$: Singular: 117 s; F_4: 25 s. $CTC_{3,4,3}$: Singular: $> 10,800$ s, F_4: $1,100$ s
- However, it is slower in (all) other cases.

DR [TF05] Idea

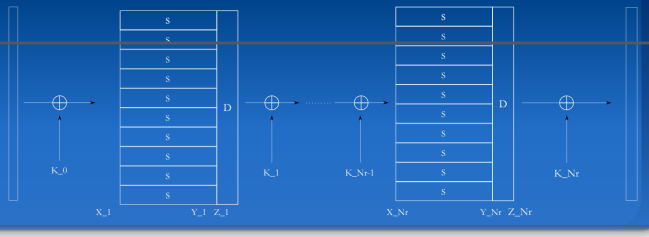


Treat one variable, say x_n, as parameter, and compute the Extended Dixon Resultant [KSY94] for the resulting system. This will result in a polynomial in one variable which vanishes at any zero of the original system. Factor the polynomial to find the roots and use that information to recover the other variables.
There is no proof that this method always holds as the RSC criterion is not proven. However, noone produced an equation system so far where the RSC criterion didn't hold.

Theorem

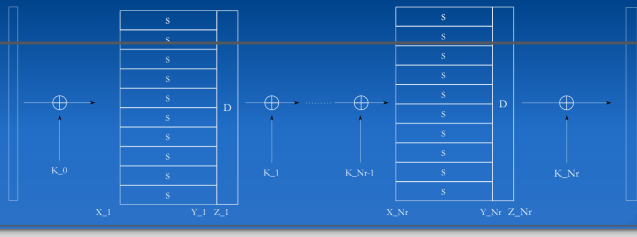
If $\exists X \in N_1$ such that $rank(X) < rank(D)$ then for all $Y \in R$, $\phi(det(Y))$ vanishes if $\phi(F)$ has a common affine zero which satisfies C.

DR Results



- Implemented DR in Singular and SAGE
- Implementation beats Singular's Gröbner basis engine for "Type A" equation systems as in [TF05].
- Slower for CTC equation systems
- The original DR [TF05] often doesn't terminate for CTC equation systems, thesis contains modified version which is guaranteed to terminate.

XL [CKPS00] Idea



For a positive integer $D \geq 2$, execute the following steps:

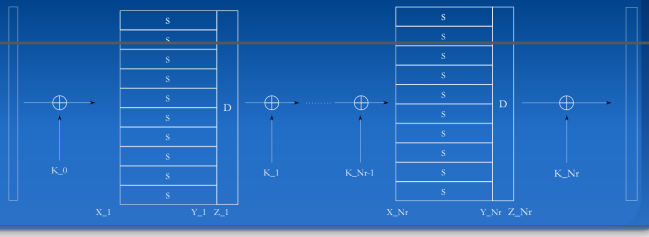
Multiply Generate all the products $\prod_{j=1}^{r} x_{i_j} \cdot f_i$ for $r \leq D - 2$.

Linearize Consider each monomial term in the x_i of degree $\leq D$ as a new indeterminate and create a system of linear equations. Perform Gaussian elimination on these linear equations, using a monomial ordering that eliminates all the terms containing one indeterminate (say, x_1) last.

Solve Assuming that step 2 yields at least one univariate equation in the powers of x_1, solve this equation over the finite field.

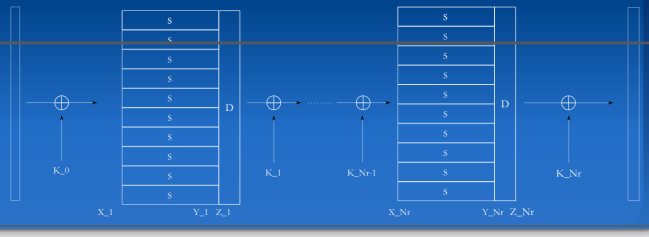
Repeat Simplify the equations and repeat the process to find the values of the other indeterminates.

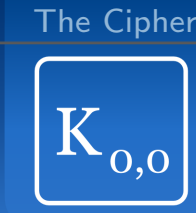
XL Results



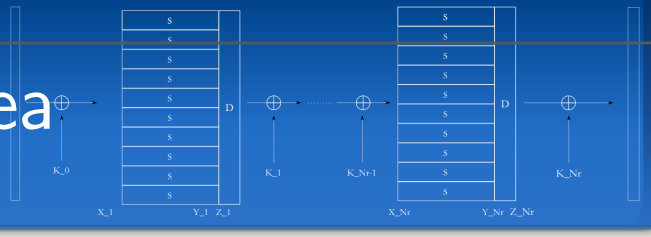
- Many variants exist for XL [Din06].
- XL is proven to be a redundant version of F_4.
- Implemented the basic version only for SAGE and this implementation is slower than Singular's Buchberger implementation.
- But CTC was broken using a "simplified and specialized" version of XL2 [YCC04] according to [CB06].

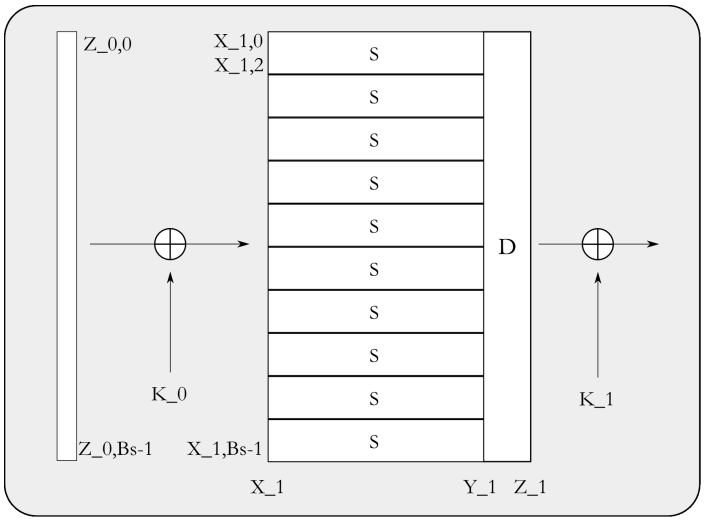
Outline

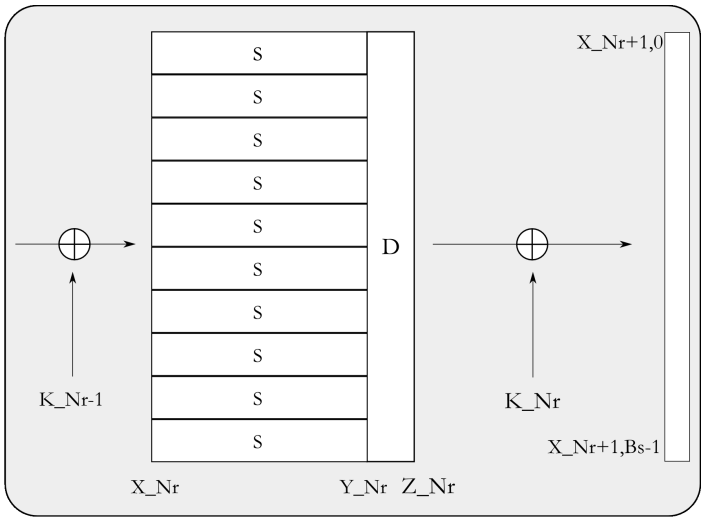




Meet-in-the-Middle [CMR05] Idea







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 $B = 2$.

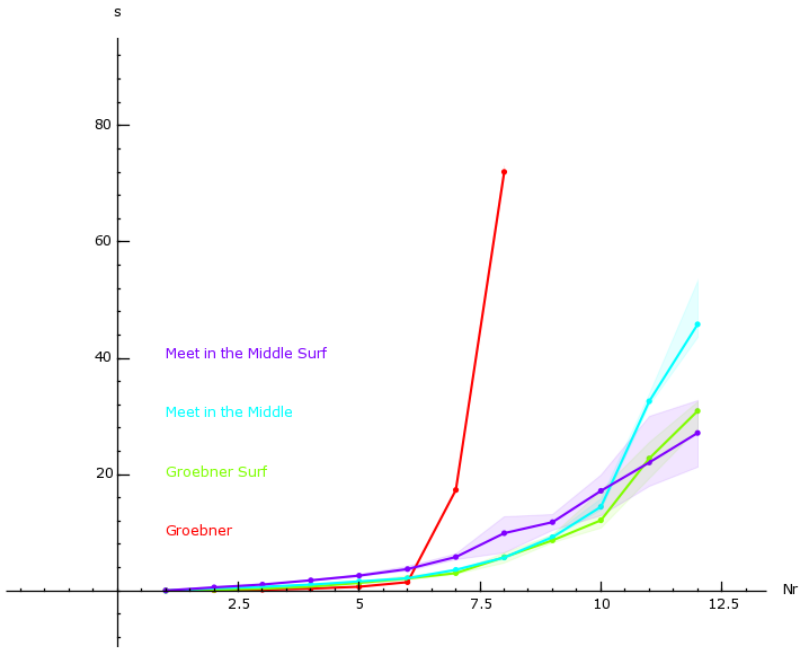
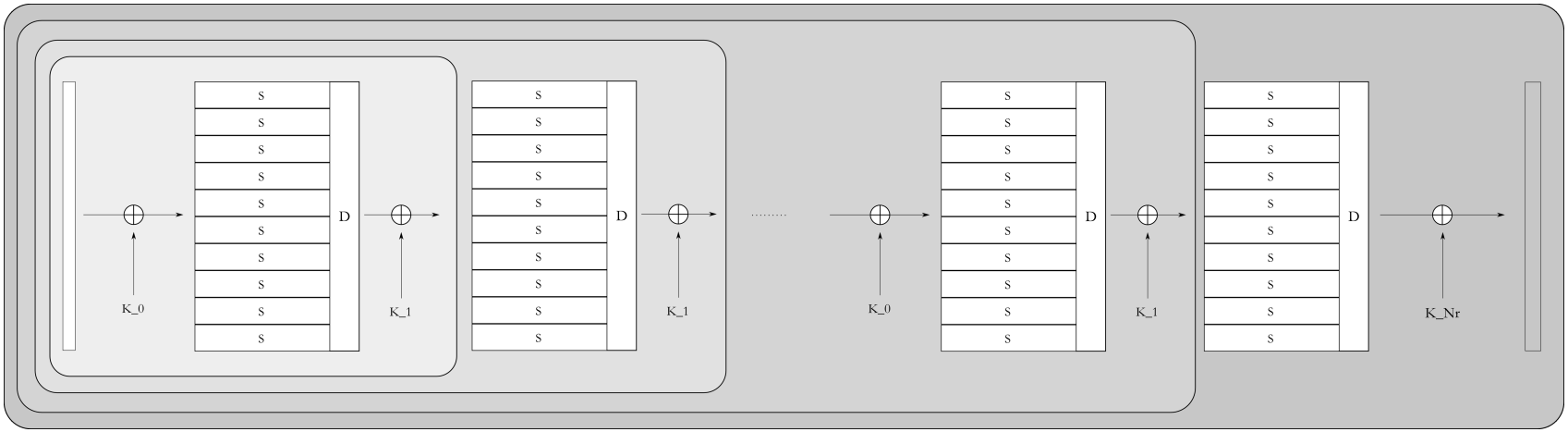
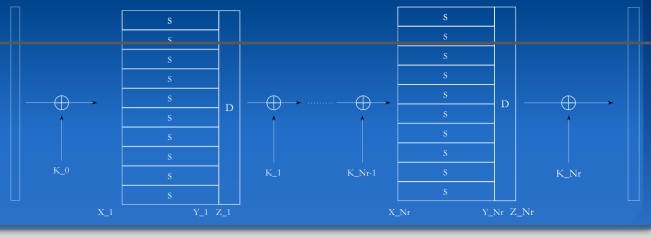


Figure: Runtimes for B=1 and term ordering *lex*

Gröbner Surfing Idea



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.

Gröbner Surfing Results II

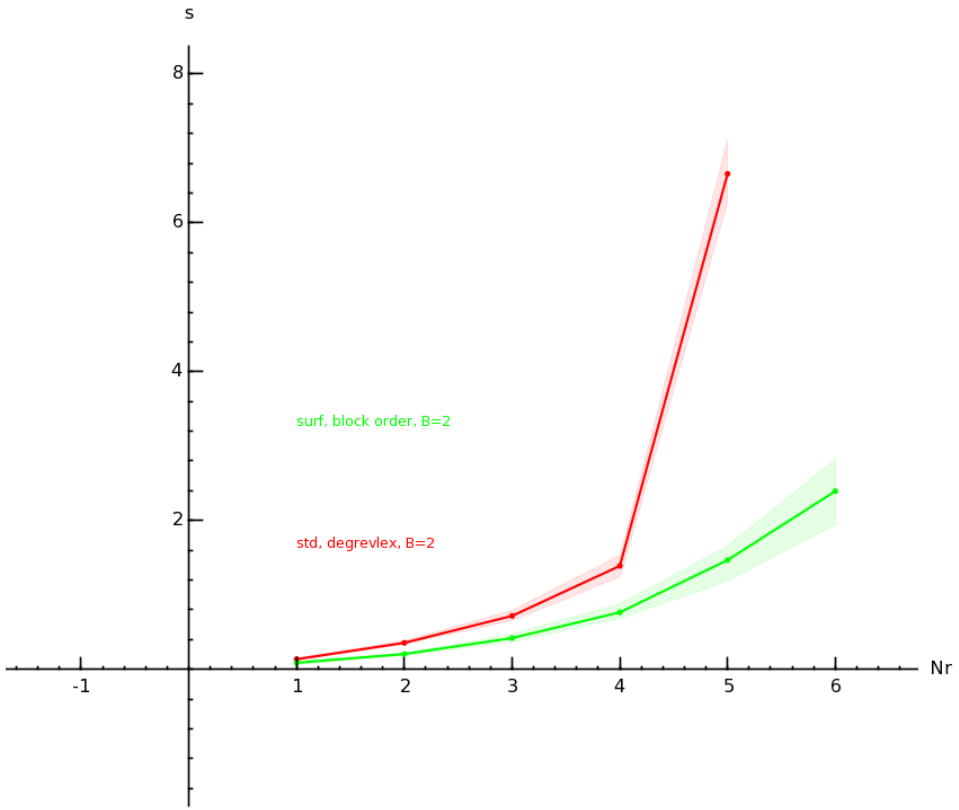


Figure: Runtimes for $B = 2$

Gröbner Surfing Results III

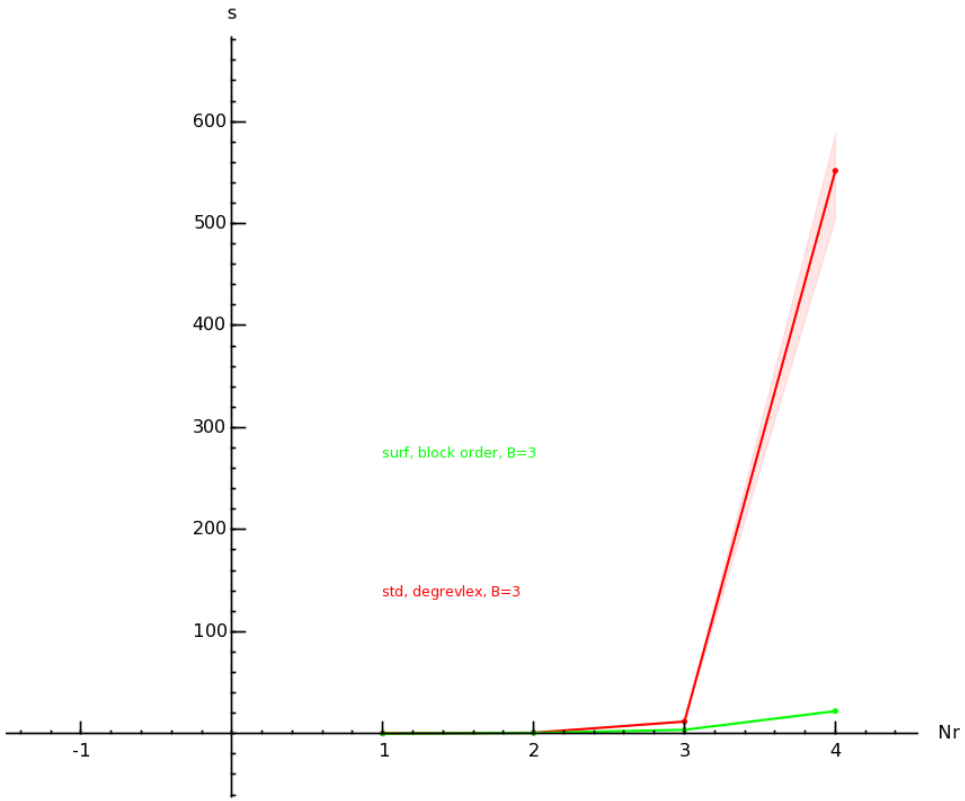
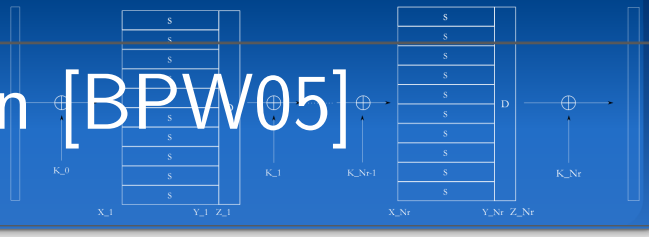


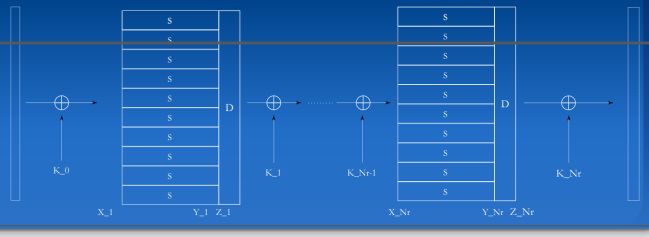
Figure: Runtimes for $B = 3$

Gröbner Basis without Reduction [BPW05]

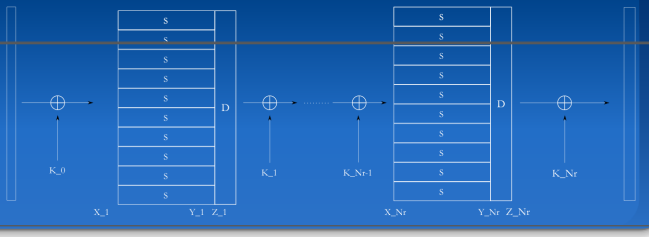


- First Buchberger Criterion: *Suppose that we have $f, g \in G$, such that the leading monomials of f and g are pairwise prime. Then the S-polynomial of f and g reduces to zero.*
- We have n equations in n variables, so make sure each leading monomial is univariate and distinct from each other.
- We 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.

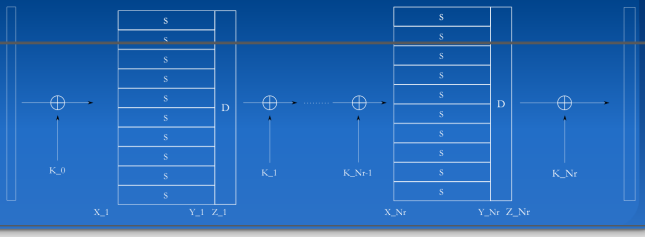
Nicolas T. Courtois and Gregory V. Bard.
Algebraic cryptanalysis of the data encryption standard.
Cryptology ePrint Archive, Report 2006/402, 2006.
available at http://http://eprint.iacr.org/2006/402.

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.

Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir.
Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations.
In *Proceedings of Eurocrypt 2000, LNCS 1807*, pages 392–407. Springer, 2000.

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.
How Fast can be Algebraic Attacks on Block Ciphers?
Cryptology ePrint Archive, Report 2006/168, 2006.
available at: http://eprint.iacr.org/2006/168.pdf.



References II

Jintai Ding.
TTM Cryptosystems and the Direct Attack Algorithms, 2006.
available at http://math.uwyo.edu/RMMC/2006/coursematerial/wyo-4.pdf.

Orr Dunkelman and Nathan Keller.
Linear Cryptanalysis of CTC.
Cryptology ePrint Archive, Report 2006/250, 2006.
available at: http://eprint.iacr.org/2006/250.pdf.

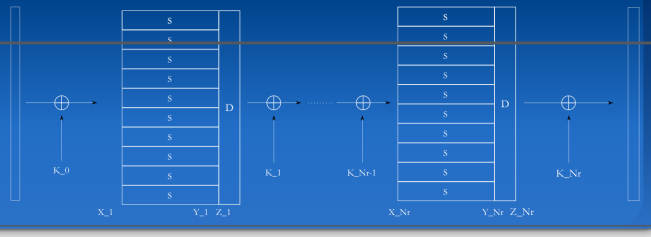
Jean-Charles Faugère.
A New Efficient algorithm for Computing Gröbner Basis (F4), 1999.
available at http://modular.ucsd.edu/129-05/refs/faugere_f4.pdf.

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.

G.-M. Greuel, G. Pfister, and H. Schönemann.
Singular 3.0.
A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005.
available at: http://www.singular.uni-kl.de.

Deepak Kapur, Tushar Saxena, and Lu Yang.
Algebraic and Geometric Reasoning using Dixon Resultants.
In *ISSAC '94: Proceedings of the international symposium on Symbolic and algebraic computation*, pages 99–107, New York, NY, USA, 1994. ACM Press.

References III



William Stein and David Joyner.

SAGE: System for Algebra and Geometry Experimentation.
In *Comm. Computer Algebra*, volume 39, pages 61–64. 2005.
available at `http://modular.ucsd.edu/sage`.

Xijin Tang and Yong Feng.

A New Efficient Algorithm for Solving Systems of Multivariate Polynomial Equations.
Cryptology ePrint Archive, Report 2005/312, 2005.
available at `http://eprint.iacr.org/2005/312`.

Ralf-Philipp Weinmann.

Private communication, 12 2006.

Bo-Yin Yang, Jiun-Ming Chen, and Nicolas T. Courtois.

On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis.
In *Proceedings of Information and Communications Security; 6th International Conference 2004, LNCS 3269*, pages 401–413. Springer, 2004.