# Algebraic Cryptanalysis using Gröbner Bases
## an introduction


Jan Ferdinand Sauer

ferdinand@asdm.gmbh


slides: asdm.gmbh/ac_using_gbs


AS Discrete Mathematics


proud to be sponsored by

ethereum foundation

# Outline – What you're getting into

1. Derive Polynomial Equations
3.
2. Gröbner Bases – Mathematical
4. Gröbner Bases – Computational
5. Term Order Change

# Motivation – A Brief History of Jarvis

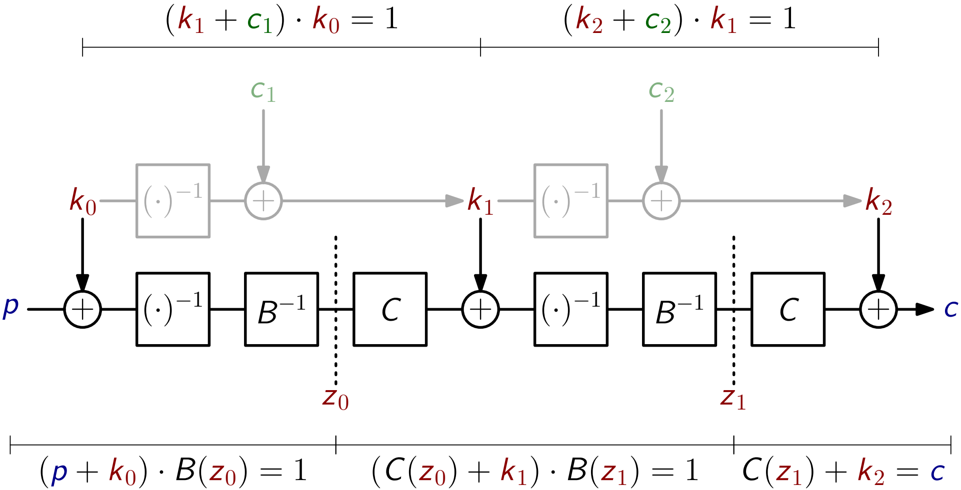
Oct '18 — Jarvis proposal

> *"Gröbner basis attacks never work."* —Tomer

Apr '19 — Jarvis attack

> *"I am probably the first symmetric-key designer to be f—d by a Gröbner basis attack."* —Tomer

# Deriving Equations – Just A Rather Variate polynomIal System



# Gröbner Bases – Polyterms and -nomials

$$\overbrace{\underbrace{3 \cdot xy}_{\text{leading term}} + \underbrace{5}_{\text{coeff}} \cdot \underbrace{yz^2}_{\text{monomial}}}^{\text{polynomial}}$$

# Gröbner Bases – I said "order!"

**Lex**icographic

$$x_1 \succ x_2 \succ \cdots \succ x_{n-1} \succ x_n$$

$$x^3 \succ x^2 z^2 \succ y^1 z^4 \succ z^5$$

**Deg**ree**rev**erse**lex**icographic

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \succ x_1^{\beta_1} \cdots x_n^{\beta_n}$$

if $\sum \alpha_i > \sum \beta_i$
reverse lex breaks ties

$$x^3 \prec x^2 z^2 \prec y^1 z^4 \succ z^5$$

# Gröbner Bases – Who's leading now?

$$\underbrace{3 \cdot xy}_{\mathrm{LT}_{\text{lex}}} + \underbrace{5 \cdot yz^2}_{\mathrm{LT}_{\text{degrevlex}}}$$

$$f \text{ div } G:$$

$$f = q_1 g_1 + \ldots + q_m g_m + r$$

# Gröbner Bases – Ideal for ideals

$$
\begin{aligned}
I &= \langle g_1, \ldots, g_m \rangle \\
&= q_1 g_1 + \ldots + q_m g_m
\end{aligned}
$$

# Gröbner Bases – Ideally defined

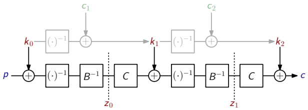
### Definition (by Leading Terms)

$G$ is Gröbner Basis $\quad\Leftrightarrow\quad \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle = \mathrm{LT}(I)$

### Definition (by Unique Remainder)

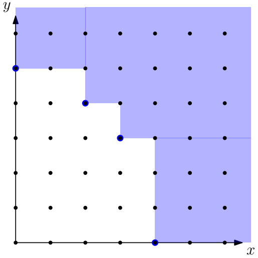
$G$ is Gröbner Basis $\quad\Leftrightarrow\quad$ $f$ div $G$ has unique remainder

# Gröbner Bases and Crypto Systems – The (missing?) link




multivariate polynomial equations

unique ideal representation




define ideal

represent ideal well

# Gröbner Bases and Crypto Systems – They've got your back-substitute

$$G_{\text{lex}} = \left\{ \begin{array}{l} x^2 - 5xyz + 5 \\ y^2 - 5z + 5 \\ z^2 - z + 4 \end{array} \right\}$$

$z=12$:

$$\left\{ \begin{array}{l} x^2 + 8xy + 5 \\ y^2 - 4 \end{array} \right\}$$

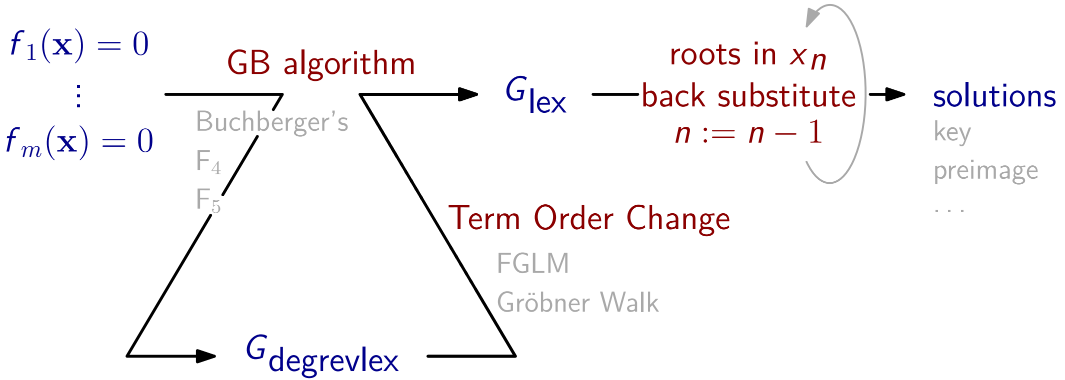
- $y=15$: $\{ x^2 + x + 5 \}$
- $y=2$: $\{ x^2 - x + 5 \}$

$z=6$:

$$\left\{ \begin{array}{l} x^2 + 4xy + 5 \\ y^2 - 8 \end{array} \right\}$$

- $y=12$: $\{ x^2 - 3x + 5 \}$
- $y=5$: $\{ x^2 + 3x + 5 \}$

# Gröbner Bases and Crypto Systems – And now follow the link



# Buchberger's Algorithm – Syzygy pylynymyals

## Example

$$S(\underbrace{3xy + \boxdot}_{f}, \underbrace{2yz + \circledcirc}_{g}) \quad = \quad \frac{xyz}{3xy} \cdot f - \frac{xyz}{2yz} \cdot g \quad = \quad \frac{z}{3} \cdot \boxdot - \frac{x}{2} \cdot \circledcirc$$

## Definition (S-Polynomial)

$$S(f, g) = \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} \cdot f - \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} \cdot g$$

## Definition (Buchberger's Criterion)

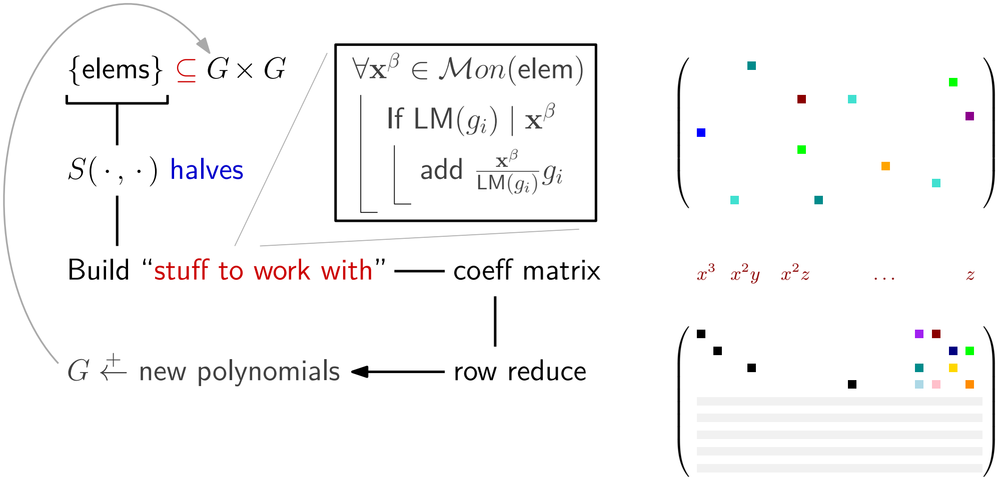
$G$ is Gröbner Basis $\quad \Leftrightarrow \quad S(g_i, g_j)$ div $G = 0$ for all pairs from $G$

# Buchberger's Algorithm – Are we there yet?

**Input:** $F = \{f_1, \ldots, f_m\}$
**Output:** Gröbner Basis $G$

$G' = F$
$G = \emptyset$
**while** $G \neq G'$ **do**
    $G = G'$
    **foreach** $(g_i, g_j) \in G \times G$ **do**
        **if** $S(g_i, g_j)$ *div* $G \neq 0$ **then** $G' \stackrel{+}{\leftarrow} S(g_i, g_j)$ div $G$
**return** $G'$

# $F_4$ – Everything at once



# $F_5$ – Your signature here, please

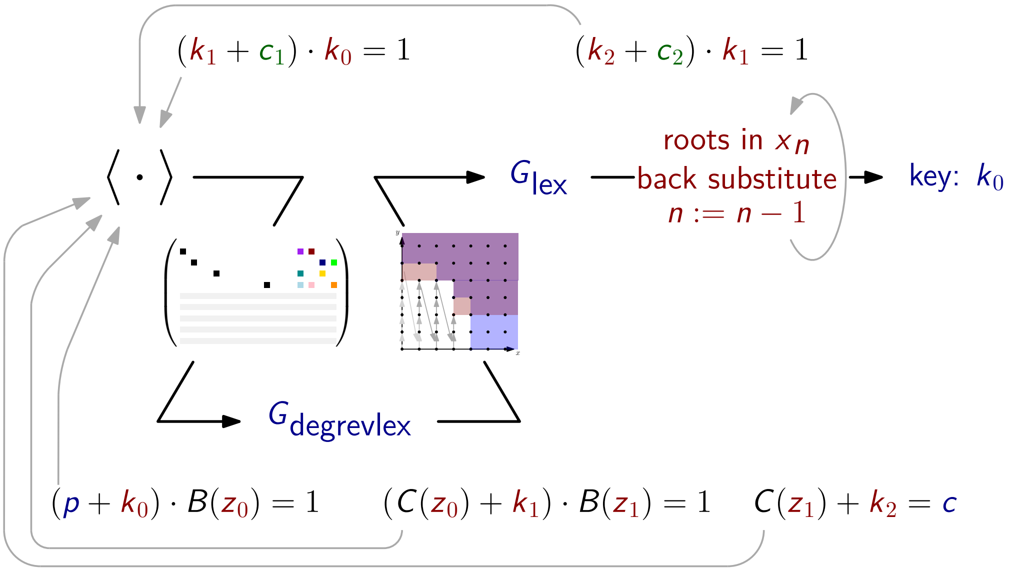
vector of origin

$$\left.\begin{matrix} f_1(\mathbf{x}) & \cdot & q_1(\mathbf{x}) \\ \vdots & & \vdots \\ f_m(\mathbf{x}) & \cdot & q_m(\mathbf{x}) \end{matrix}\right\} \sum = g$$

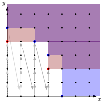
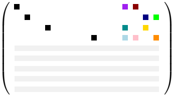
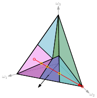
signatures

$$\begin{pmatrix} x^2y + y \\ xy^2 \\ y^2 + yz \\ 0 \end{pmatrix} \xrightarrow{\mathfrak{s}} \begin{pmatrix} 0 \\ 0 \\ y^2 \\ 0 \end{pmatrix}$$

# Summary – This is a wrap



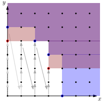
# Complexities – Computational, not mental

| | | | |
|---|---|---|---|
| $\forall S({\color{red}g_i}, {\color{blue}g_j})$ | $\mathcal{O}_{\text{worst}}\left(d_{\max}^{2^{n+o(1)}}\right)$ <br> $\mathcal{O}_{\text{avg}}\left(d_{\max}^{3n}\right)$ |  | $\mathcal{O}\left(n \cdot \dim_{\mathbb{F}_q}(R/I)^3\right)$ |
|  | $\mathcal{O}\left(m\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$ |  | ? |
| $\mathfrak{S}$ | $\mathcal{O}\left(m\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$ | roots in $x_n$ <br> back substitute <br> $n := n-1$ | $\mathcal{O}(d_{\max}^2 \log d_{\max} \log q)$ |

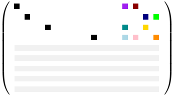
# Further reading – The NeverEnding Story

$\forall S(g_i, g_j)$

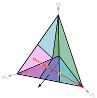
Ideals, Varieties, and Algorithms
*Cox et. al.*



Using Algebraic Geometry
*Cox et. al.*



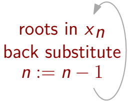
Ideals, Varieties, and Algorithms
*Cox et. al.*



Using Algebraic Geometry
*Cox et. al.*

$\mathfrak{S}$

A Survey on Signature-Based Gröbner Basis Computations
*Eder & Faugère*




Modern Computer Algebra
*von zur Gathen et. al.*