On the relation of the Mutant strategy and the Normal Selection strategy

Martin Albrecht[1] Carlos Cid[2] Jean-Charles Faugère[1] Ludovic Perret[1]

1 SALSA Project -INRIA, UPMC, Univ Paris 06
2 Information Security Group, Royal Holloway, University of London

20.1.2011

Outline

1. Motivation
2. Gröbner Basics
3. Mutants
4. Mutants in MXL_3
5. MXL_3 and the Normal Selection Strategy

Outline

Polynomial System Solving

- Polynomial system solving has many applications in cryptography, mainly in cryptanalysis.
- In particular, the security of many cryptographic primitives can be related to solving large systems of equations.
- Thus, studying the complexity of and algorithms for solving such systems is an important task for cryptographers.
- However, much of the research in this direction in the cryptographic community is done without taking the theory of polynomial system solving from commutative algebra into sufficient consideration.
- The prime example of this missing connection is the XL algorithm for solving multivariate polynomial systems of equations.

XL and F4

- It is well-known that the XL algorithm [CKPS00] is a redundant variant of the F_4 [Fau99] algorithm for computing Gröbner bases [AFI$^+$04].
- The "Mutant XL" series of algorithms has attracted attention from the cryptographic community since
  - practical implementations offer good performance w.r.t. some metrics and
  - the concept of "Mutants" promises a new direction on polynomial system solving.

It is thus natural to ask what Mutants are exactly and whether we can understand them in the context of commutative algebra.

Outline

Notation I

- $R = \mathbb{F}[x_0, \ldots, x_{n-1}]$, we assume a degree term ordering in this work.
- T denotes the set of all monomials in R.
- Let $m = x^{\alpha(i)} = x_0^{\alpha_0} x_1^{\alpha_1} \ldots x_{n-1}^{\alpha_{n-1}}$. We define the **exponent vector**:

$$\text{expvec}(m) = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}).$$

- $\mathrm{LM}(f)$ is the largest or leading monomial appearing in f.
- $\mathrm{LM}(F) = \{\mathrm{LM}(f) \mid f \in F\}$.
- $\mathrm{LC}(f)$ is the coefficient corresponding to $\mathrm{LM}(f)$ in f.
- $\mathrm{LT}(f)$ is $\mathrm{LC}(f)\mathrm{LM}(f)$.
- $\mathrm{LV}(f)$ denotes the biggest variable in $\mathrm{LM}(f)$.
- $\mathrm{LV}(F, x)$ is defined as $\{f \in F, \mathrm{LV}(f) = x\}$.
- We denote by $S_{(op)d}$ the subset of S with elements of degree $(op)d$ where $(op) \in \{=, <, \leq, >, \geq\}$.

Notation II

An example in $\mathbb{F}[x, y, z]$ with term ordering **deglex**:

$$f = 3yz + 2x + 1$$

- $\mathrm{LM}(f) = yz$,
- $\mathrm{LC}(f) = 3$,
- $\mathrm{LT}(f) = 3yz$ and
- $\mathrm{LT}(f) = y$.

Notation III

We may write multiples of polynomials $f_0, \ldots, f_{m-1}$ in "matrix notation":

$$\begin{array}{c} \\ (t_{0,0}, f_0) \\ (t_{0,1}, f_0) \\ (t_{0,2}, f_0) \\ \vdots \\ (t_{1,0}, f_1) \\ \vdots \\ (t_{m-1,0}, f_{m-1}) \\ (t_{m-1,1}, f_{m-1}) \\ \vdots \end{array} \quad \begin{array}{c} \text{monomials of degree } D \\ \left(\begin{array}{ccc} \quad & \quad & \quad \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \right) \end{array}$$

Notation IV

Definition

Let $f_0, \ldots, f_{m-1}$ be polynomials in R. The set

$$\langle f_0, \ldots, f_{m-1} \rangle = \left\{ \sum_{i=0}^{m-1} h_i f_i \mid h_0, \ldots, h_{m-1} \in R \right\}.$$

is an ideal. This ideal is called the ideal generated by $f_0, \ldots, f_{m-1}$.

Notation V

Definition (Gröbner Basis)

Let $\mathcal{I}$ be an ideal of $\mathbb{F}[x_0, \ldots, x_{n-1}]$ and fix a monomial ordering. A finite subset

$$G = \{g_0, \ldots, g_{m-1}\} \subset \mathcal{I}$$

is said to be a **Gröbner basis** of $\mathcal{I}$ if

$$\forall f \in \mathcal{I} \text{ there exists } g_i \in G \text{ such that } \mathrm{LM}(g_i) \mid \mathrm{LM}(f).$$

Notation VI

Definition (Reduced Gröbner Basis)

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

1. $\mathrm{LC}(f) = 1$ for all $f \in G$;
2. $\forall f \in G, \nexists\ m \in M(f)$ such that $m \in \langle \mathrm{LM}(G \setminus \{f\}) \rangle$.

Notation VII

- Computing the reduced Gröbner basis from any Gröbner basis is a polynomial time algorithm in the size of th basis.
- The reduced Gröbner basis is unique for a given ideal and term ordering.
- Let $c = c_0, \ldots, c_{n-1}$ be the unique solution for all

  $$f \in \mathcal{I} = \langle f_0, \ldots, f_{n-1} \rangle.$$

  Then, the reduced Gröbner basis is

  $$x_0 - c_0, \ldots, x_{n-1} - c_{n-1}.$$

- Thus, if a system of equations has exactly one solution then computing the Gröbner basis is equivalent to computing this solutions.

S-polynomials I

Bruno Buchberger proved in his PhD thesis [Buc65] that Gröbner bases can be computed by considering S-polynomials.

Definition (S-Polynomial)

Let $f, g \in \mathbb{F}[x_0, \ldots, x_{n-1}]$ be non-zero polynomials.

- Let x^γ be the least common multiple of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, written as
$$x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g)).$$
- The S-polynomial of f and g is defined as
$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

S-polynomials II

For example, in $\mathbb{F}[x, y, z]$ with a deglex term ordering the S-polynomial of $f = xy + x + 1$ and $g = yz + x$ is

$$zf - xg = \mathbf{xyz} + xz + z - \mathbf{xyz} - x^2 = -x^2 + xz + z.$$

S-polynomials III

In fact, it is **sufficient** to consider **only** S-polynomials in Gröbner basis computations since **any** reduction of leading terms can be attributed to S-polynomials.

S-polynomials IV

Consider

$$f = \sum_{i=0}^{t-1} c_i m_i f_i$$

where m_i is some monomial and assume

$$\mathrm{LM}(f) < \min\{\mathrm{LM}(m_i f_i) \mid 0 \leq i < t\}$$

i.e. that we have cancellations of leading terms.

These cancellations can be attributed to S-polynomials.

S-polynomials V

Lemma (Cancellation, [CLO92])

Let every element of $f = \Sigma_{i=0}^{t-1} c_i x^{\alpha(i)} f_i$ *and constants* $c_0, \ldots, c_{n-1}$ *have exponent vector* δ *if* $c_i \neq 0$*, that is* $\alpha(i) + \text{expvec}(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$*. If the sum* f *has a smaller leading exponent vector, then there exists constants* c_{jk} *such that*

$$\sum_{i=0}^{t-1} c_i x^{\alpha(i)} f_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(f_j, f_k) \quad (1)$$

where $x^{\gamma_{jk}} = \mathrm{LCM}(\mathrm{LM}(f_j), \mathrm{LM}(f_k))$*.*

Furthermore, each $x^{\delta-\gamma_{jk}} S(f_j, f_k)$ *has a leading exponent vector* $< \delta$*.*

S-polynomials VI

Let $f_{jk} = x^{\delta - \gamma_{jk}} S(f_j, f_k)$. Note that the claim of the Cancellation Lemma is **not** that

$$\mathrm{LM}(f_{jk}) \leq \mathrm{LM}(f),$$

instead the claim is that the representation gets **smaller** ("$< \delta$").

However, computing S-polynomials of S-polynomials, i.e. a repeated application of the Cancellation Lemma to $f = \Sigma_{ij} c_{jk} x^{\alpha(jk)} f_{jk}$ if $\mathrm{LM}(f) < \mathrm{LM}(x^{\delta - \gamma_{jk}} S(f_j, f_k))$ will produce a representation which is minimal.

S-polynomials VII

Thus, whatever cancellations can be produced by monomial multiplies and $\mathbb{F}$-linear combinations, they can be attributed to S-polynomials.

Consequently, the only cancellations that need to be considered in an XL style algorithm are those produced by S-polynomials.

Example I

Consider the polynomials in $\mathbb{F}_{127}[x, y, z]$ with term ordering deglex:

$$
\begin{aligned}
f &= xy + x + 1, \\
g &= x + 1 \text{ and} \\
h &= z + 1.
\end{aligned}
$$

We can construct two S-polynomials of degree two:

$$
\begin{aligned}
s_0 = \quad & f - yg & = x - y + 1 \text{ and} \\
s_1 = \quad & zg - xh & = -x + z.
\end{aligned}
$$

In matrix notation we thus need at most 6 rows: f, yg, zg, yh, g, h.

Example II

For comparison, XL would consider the following nine polynomials up to degree two.

$$
\begin{aligned}
f &= xy + x + 1, \\
xg &= x^2 + x, \\
yg &= xy + y, \\
zg &= xz + z, \\
xh &= xz + x, \\
yh &= yz + y, \\
zh &= z^2 + z, \\
g &= x + 1 \text{ and} \\
h &= z + 1.
\end{aligned}
$$

Example III

In matrix notation:

$$\begin{pmatrix} 0&1&0&0&0&1&0&0&1\\ 1&0&0&0&0&1&0&0&0\\ 0&1&0&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&1&0\\ 0&0&1&0&0&1&0&0&0\\ 0&0&0&1&0&0&1&0&0\\ 0&0&0&0&1&0&0&1&0\\ 0&0&0&0&0&1&0&0&1\\ 0&0&0&0&0&0&0&1&1 \end{pmatrix} \rightarrow \begin{pmatrix} 1&0&0&0&0&0&0&0&-1\\ 0&1&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&-1\\ 0&0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&-1\\ 0&0&0&0&0&1&0&0&1\\ 0&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1&1\\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}$$

The **rank** is **eight**; yet, we know from the Cancellation Lemma that **six** rows (f, yg, zg, yh, g, h) would have been sufficient.

Example IV

- Furthermore, from Buchberger's first criterion [CLO92] we know that only the four rows f, yg, g, h need to be considered since the leading terms of g and h are pairwise prime.
- Thus, the matrix constructed by XL contains 4 out of 9 rows which are **redundant** even though they **do not reduce to zero**.
- Conversely, any reduction that produced a new lower leading term in the matrix constructed by XL can be attributed to S-polynomials.

Another Example I

S-polynomials of S-polynomials

Consider the polynomials $f = xy + a$, $g = yz + b$, and $h = ab + 1$.

- Only one S-polynomial does not reduce to zero: $s_0 = zf - xg = za - xb$.
- From s_0 we can then construct $s_1 = bs_0 - zh = xb^2 + z$ also at degree three which is an element of the Gröbner basis.
- XL at degree 3 will produce

  $$\{m \cdot p \mid m \in \{1, x, y, z, a, b\}, p \in \{f, g, h\}\}$$

  which reduces to $x^2y + xa$, $xy^2 + ya$, $xyz + xb$, $y^2z + yb$, $yz^2 + zb$, $xya + a^2$, $yza - 1$, $xyb - 1$, $yzb + b^2$, $xab + x$, $yab + y$, $zab + z$, $a^2b + a$, $ab^2 + b$, $xy + a$, $yz + b$, $za - xb$ and $ab + 1$.
- Note that $xb^2 + z$ is not in that list.

Another Example II

S-polynomials of S-polynomials

- However, if we increase the degree of XL to four, the list that is returned is $x^3y + x^2a$, $x^2y^2 - a^2$, $xy^3 + y^2a$, $x^2yz + x^2b$, $xy^2z + 1$, $y^3z + y^2b$, $xyz^2 + xzb$, $y^2z^2 - b^2$, $yz^3 + z^2b$, $x^2ya + xa^2$, $xy^2a + ya^2$, $xyza - x$, $y^2za - y$, $yz^2a - z$, $xya^2 + a^3$, $yza^2 - a$, $x^2yb - x$, $xy^2b - y$, $xyzb - z$, $y^2zb + yb^2$, $yz^2b + zb^2$, $x^2ab + x^2$, $xyab - a$, $y^2ab + y^2$, $xzab + xz$, $yzab - b$, $z^2ab + z^2$, $xa^2b + xa$, $ya^2b + ya$, $za^2b + xb$, $a^3b + a^2$, $xyb^2 - b$, $yzb^2 + b^3$, $xab^2 + xb$, $yab^2 + yb$, $zab^2 + zb$, $a^2b^2 - 1$, $ab^3 + b^2$, $x^2y + xa$, $xy^2 + ya$, $xyz + xb$, $y^2z + yb$, $yz^2 + zb$, $xya + a^2$, $xza - x^2b$, $yza - 1$, $z^2a - xzb$, $za^2 + x$, $xyb - 1$, $yzb + b^2$, $xab + x$, $yab + y$, $zab + z$, $a^2b + a$, $\mathbf{xb^2 + z}$, $ab^2 + b$, $xy + a$, $yz + b$, $za - xb$ and $ab + 1$.
- XL could not produce $xb^2 + z$ at degree 3 since this element corresponds to

$$b(zf - xg) - zh = (bz)f - (bx)g - zh,$$

but we have that $\deg(bzf) = 4$.

Outline

Definition I

Let $\mathcal{I} = \langle f_0, \ldots, f_{m-1} \rangle \subset \mathbb{F}[x_0, \ldots, x_{n-1}]$. Any element element $f \in \mathcal{I}$ can be written as:

$$f = \sum_{f_i \in F} h_i \cdot f_i, \text{ with } h_i \in \mathbb{F}[x_0, \ldots, x_{n-1}].$$

- We call **level** of the representation $\sum_{f_i \in F} h_i \cdot f_i$ of $f \in \mathcal{I}$ the maximum degree of $\{h_i \cdot f_i \mid f_i \in F\}$.
- We call **level** of f the minimal level of all its representations.

Definition II

Definition

A polynomial $f \in \mathcal{I}$ is a **mutant** *if its total degree is strictly less than its level.*

In the language of commutative algebra, a mutant occurs when an S-polynomial has a lower degree leading term after reduction by the basis F which was not in F before reduction.

Outline

Pseudocode

begin

$d \longleftarrow \min\{\deg(f) \mid f \in F\}$;

$M \longleftarrow \varnothing$;

while True do

$\tilde{F}_{\leq d} \longleftarrow$ the row echelon form of $F_{\leq d}$;

$M \longleftarrow M \cup \{f \in \tilde{F}_{\leq d} \mid \deg(f) < d$ **and** $\mathrm{LM}(f) \notin \mathrm{LM}(F_{\leq d})\}$;

$F_{\leq d} \longleftarrow \tilde{F}_{\leq d}$;

if $M \neq \varnothing$ **then**

$k, y \longleftarrow \min\{\deg(f) \mid f \in M\}, \max\{\mathrm{LV}(f) \mid f \in F_{\leq k+1}\}$;

$M_{=k}^{+} \longleftarrow$ Multiply all elements of $M_{=k}$ by all variables $\leq y$;

$M, F \longleftarrow M \setminus M_{=k}, F \cup M_{=k}^{+}$;

$d \longleftarrow k + 1$;

$\ldots$

end

Simplified F_4

begin

$G, i, \tilde{F}_i^+ \longleftarrow F, 0, F$; $P \longleftarrow \{\textsc{Pair}(f,g) : \forall f, g \in G$ **with** $g > f\}$;

while $P \neq \varnothing$ **do**

$i \longleftarrow i+1$; $P_i \longleftarrow \textsc{Sel}(P)$; $P \longleftarrow P \setminus P_i$;

$F_i \longleftarrow \{t \cdot f, \forall (t,f) \in \text{Left}(P_i) \bigcup \text{Right}(P_i)\}$;

$Done \longleftarrow \mathrm{LM}(F_i)$;

while $M(F) \neq Done$ **do**

$m \longleftarrow$ an element in $M(F) \setminus Done$;

add m to $Done$;

if $\exists\, g \in G : \mathbf{LM}(g) \mid m$ **then** add $m/\mathrm{LM}(g) \cdot g$ to F_i;

$\tilde{F}_i \longleftarrow$ the row echelon form of F_i;

for $h \in \{f \in \tilde{F}_i \mid \mathbf{LM}(f) \notin \mathbf{LM}(F)\}$ **do**

$P \longleftarrow P \bigcup \{\textsc{Pair}(f,h) : \forall f \in G\}$;

add h to G;

return G;

end

Outline

Mutants I

In MXL_3 instead of increasing the degree d in each iteration, if there is a fall of degree then these new elements are treated at the current or perhaps a smaller degree before the algorithm proceeds to increase the degree.

Thus, compared to XL the MXL family of algorithms may terminate at a lower degree.

Note, we ignore the partial enlargement strategy for now.

Mutants II

The F_4 algorithm does not specify how to choose polynomials in each iteration of the main loop.

Instead, the user passes a function $\textsc{Sel}$ which specifies how to select critical pairs. In [Fau99] it is suggested to choose the pairs according to lowest degree similar to the **Normal Selection Strategy** in Buchberger's algorithm.

Mutants III

Definition (Normal Strategy in F_4)

Let $\mathcal{P}$ be a tuple of critical pairs and let $\mathrm{LCM}(p_{ij})$ denote the least common multiple of the leading monomials of the two parts of the critical pair $p_{ij} = (f_i, f_j)$.

Further, let $d = \min\{\deg(\mathrm{LCM}(p)), p \in \mathcal{P}\}$ denote the minimal degree of those least common multiples of p in $\mathcal{P}$.

Then the normal selection strategy selects the subset $\mathcal{P}'$ of $\mathcal{P}$ with $\mathcal{P}' = \{p \in \mathcal{P} \mid \deg(\mathrm{LCM}(p)) = d\}$.

Mutants IV

Theorem

Assume that $M \neq \varnothing$ in MXL_3. The set of polynomials $F_{\leq k+1}$ considered in the next iteration of the loop is a superset of the polynomials considered by F_4 when using the **Normal Selection Strategy** *in the iteration $i+1$ if up to this point MXL_3 computed a superset of the polynomials of F_4. Furthermore, every polynomial $\in F_{\leq k+1}$ not in the set considered by F_4 is redundant at this step.*

Mutants V

Proof:

- If $\textsc{Sel}$ is the Normal Selection Strategy, the set $\mathcal{P}_{i+1}$ will contain the S-polynomials of lowest degree in $\mathcal{P}$.
- Every S-polynomial in $\mathcal{P}_{i+1}$ will have at least degree $k+1$, since the set $M_{=k}$ is in row echelon form and k is the minimal degree in M.
- If there exists an S-polynomial of degree $k+1$ then it is of the form $t_i f_i - t_j f_j$ with $\deg(t_i f_i) = k+1$ and $\deg(t_j f_j) = k+1$, where at least one of t_i, t_j has degree 1.
- Since MXL_3 constructs all multiples $t_{ij} f_i$ with $\deg(t_{ij}) = 1$ if $\deg(f_i) = k$ and includes all elements of degree $k+1$ which can be produced in the next iteration, both components of the S-polynomial are included in $F_{\leq k+1}$.

Mutants VI

- In the **Symbolic Preprocessing** phase F_4 also constructs all components of **potential** S-polynomials that could arise during the elimination.
- These are always of the form $f_i - t_j f_j$ where $\deg(f_i) = \deg(t_j f_j)$.
- Since MXL_3 considers all monomial multiplies of all f_j up to degree $k+1$ in the next iteration, these components are also included in the set F_{k+1}.

Mutants VII

- Recall from the Cancellation Lemma that all $f = \Sigma_{i=0}^{t-1} c_i x^{\alpha(i)} f_i$ can be rewritten as

$$f = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(f_j, f_k).$$

- Note that $\deg(x^{\delta}) \leq k+1$ for $F_{\leq k+1}$ and that $\deg(x_{jk}^{\gamma}) = k+1$ for all S-polynomials contained in $F_{\leq k+1}$. We thus have that $\deg(x^{\delta - \gamma_{jk}}) = 0$ if $c_{jk} \neq 0$.

Mutants VIII

- Consequently, any element f with smaller leading term that can be produced by $\mathbb{F}$-linear combinations of elements in $F_{\leq k+1}$ can be reduced to an $\mathbb{F}$-linear combination of S-polynomials.
- Thus, it follows from the Cancellation Lemma that any multiple of f_i which does not correspond to an S-polynomial is redundant at this step since it cannot lead to a drop of a leading monomial. $\square$

Partitioning I

The Partial enlargement technique was introduced in MXL_2 and applied in MXL_3. Instead of multiplying every polynomial $f_i \in F$ by all variables in $\mathbb{F}[x_0, \ldots, x_{n-1}]$ only a subset $\mathrm{LV}(F, x)$ is considered, where x increases with every iteration if no Mutants were founds.

Partitioning II

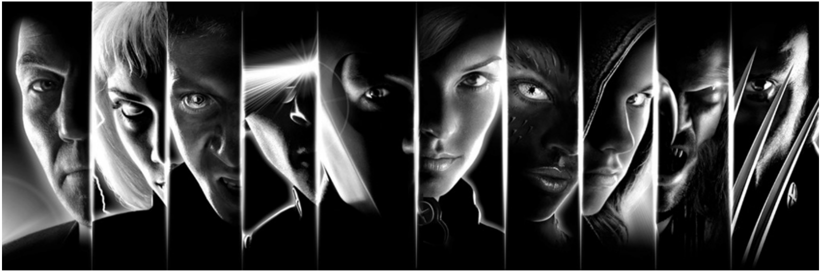
- This corresponds to selecting a subset of S-polynomials of minimal degree in SEL instead of selecting all polynomials of minimal degree.
- For example, both POLYBORI [BD07] and MAGMA [BCP97] provide an option to restrict the number of S-polynomials considered in each iteration using some fixed constant.
- However, the strategies how to select a subset are slightly different.
  - Both strategies always pick the smallest S-polynomials.
  - MAGMA and POLYBORI pick up to a fixed number of S-polynomials
  - MXL_3 picks a variable number of S-polynomials depending on the number of S-polynomials in a given partition.

Conclusion

- We have shown, that the Mutant strategy is a redundant variant of the Normal Selection strategy as used in F_4.
- We have shown that the Partitioning or Partial Enlargement Technique used in MXL_2 and following algorithms is a equivalent to selecting a subset of S-polynomials in F_4 implementations. However, the strategy how to select the size of the subsets are different in well-known F_4 implementations and MXL_3.
- Since XL is a redundant variant of the F_4 algorithm and by mapping all novel concepts to their Gröbner basis equivalent, we conclude that the MXL family of algorithms are variants of the F_4 algorithm.

We thus expect that the performance of implementations of the MXL family of algorithms can be improved considerably by introducing the notion of critical pairs and Buchberger's criteria for avoiding useless pairs.

Thank you for your attention



Mutants are people too!

Literature I

Gwenole Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita.
Comparison between XL and Gröbner basis algorithms.
In *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, Berlin, Heidelberg, New York, 2004. Springer Verlag.

Wieb Bosma, John Cannon, and Catherine Playoust.
The MAGMA Algebra System I: The User Language.
In *Journal of Symbolic Computation 24*, pages 235–265. Academic Press, 1997.

Michael Brickenstein and Alexander Dreyer.
PolyBoRi: A framework for Gröbner basis computations with Boolean polynomials.
In *Electronic Proceedings of MEGA 2007*, 2007.
Available at
http://www.ricam.oeaw.ac.at/mega2007/electronic/26.pdf.

Literature II

Bruno Buchberger.
Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.
PhD thesis, Universität Innsbruck, 1965.

Nicolas T. Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir.
Efficient algorithms for solving overdefined systems of multivariate polynomial equations.
In *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 392–407, Berlin, Heidelberg, New York, 2000. Springer Verlag.

David Cox, John Little, and Donal O'Shea.
Ideals, Varieties, and Algorithms.
Springer Verlag, Berlin, Heidelberg, New York, 1 edition, 1992.

Literature III

Jean-Charles Faugère.
A new efficient algorithm for computing Gröbner basis (F4).
Journal of Pure and Applied Algebra, 139(1-3):61–88, 1999.