Noname manuscript No.
(will be inserted by the editor)

Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures

Boo Barkee · Michela Ceria · Theo Moriarty · Andrea Visconti

Received: date / Accepted: date

Abstract In 1994, Moss Sweedler's dog proposed a cryptosystem, known as *Barkee's Cryptosystem*, and the related cryptanalysis. Its explicit aim was to dispel the proposal of using the urban legend that "Gröbner bases are hard to compute", in order to devise a public key cryptography scheme. Therefore he claimed that "no scheme using Gröbner bases will ever work".

Later, further variations of *Barkee's Cryptosystem* were proposed on the basis of another urban legend, related to the infiniteness (and consequent uncomputability) of non-commutative Gröbner bases; unfortunately Pritchard's algorithm for computing (finite) non-commutative Gröbner bases was already available at that time and was sufficient to crash the system proposed by Ackermann and Kreuzer.

The proposal by Rai, where the private key is a principal ideal and the public key is a bunch of polynomials within this principal ideal, is surely immune to Pritchard's attack but not to Davenport's factorization algorithm. It was recently adapted specializing and extending Stickel's Diffie-Hellman protocols in the setting of Ore extension. We here propose a further generalization, point the potential cryptanalisis given by

The second author has been partially funded by INdAM - Istituto Nazionale di Alta Matematica, therefore she is thankful to this institution for its support.

Boo Barkee
Sore Bone
E-mail: 3.14159x2.71828@gmail.com

M. Ceria
Department of Computer Science - University of Milan - Via Celoria 18, 20133 Milano, Italy
Tel.: +39-02-50316361
E-mail: michela.ceria@gmail.com

Theo Moriarty
SPECTRE
E-mail: 5919@unige.it

Andrea Visconti
Department of Computer Science - University of Milan - Via Celoria 18, 20133 Milano, Italy
Tel.: +39-02-50316361
E-mail: andrea.visconti@unimi.it

the Passau result and show that such protocols can be performed simply via polynomial division.

Keywords Barkee's cryptosystem · Polly Cracker · Buchberger Theory · Stickel's protocol

1 Introduction

In 1994, Moss Sweedler's dog [6] proposed a cryptosystem – the *Barkee's Cryptosystem* – and the related cryptanalysis. Its explicit aim was to dispel the proposal of using "the fact that Gröbner bases are hard to compute, to devise a public key cryptography scheme" claiming that "no scheme using Gröbner bases will ever work". Barkee's scheme writes down an easy-to-produce Gröbner basis $F = \{f_1, \dots, f_s\}$ via Macaulay's Trick [48] generating an ideal $\mathsf{I} := \mathbb{I}(F) \subset \mathcal{P} := \mathbb{F}[X_1, \dots, X_n]$ and publishes a set $G := \{g_1, \dots, g_l\} \subset \mathbb{I}(F)$ of *dense* polynomials of degree at most d in $\mathcal{P}$ and a set $T := \{\tau_1, \dots, \tau_s\} \subset \mathbf{N}(\mathbb{I}(F)) = \mathcal{T} \setminus \mathbf{T}(\mathbb{I}(F))$ of *normal terms* "*either the whole of it, or, for added security, a subset of it*" [6] belonging to the Gröbner *éscalier* of $\mathbb{I}(F)$. In order to send a message $M := \sum_{i=1}^{s} c_i\tau_i \in \mathrm{Span}_{\mathbb{F}}(T)$, the sender produces random *dense* polynomials $p_j \in \mathcal{P}, 1 \leq j \leq l, \deg(p_i) = r$, and encrypts M as $C := M + \sum_{j=1}^{l} p_j g_j$; the receiver, possessing the Gröbner basis of $\mathbb{I}(F)$ applies Buchberger's reduction to obtain the canonical form of C: $\mathrm{Can}(C, \mathbb{I}(F)) = M = \sum_{i=1}^{s} c_i\tau_i$.

It is easy to realize that denoting, for each $\delta \in \mathbb{N}$, $\mathcal{T}_{\leq\delta} := \{\tau \in \mathcal{T} : \deg(\tau) \leq \delta\}$ and $\mathsf{T}(\delta) := \#\mathcal{T}_{\leq\delta} = \binom{\delta+n}{n}$ both encoding and decoding costs between $O(\mathsf{T}(d + r))$ (the time needed to scan a dense message) and $O(\mathsf{T}^2(d + r))$ (the cost of Buchberger's reduction algorithm in the generic case).

The point of [6] was that an enemy would have been able to read the message without even attempting to perform the hard Gröbner basis computation but with a more elementary linear-algebra based approach. Namely the authors proposed two attacks, one based on [22], with complexity $O(\mathsf{T}^4(d + r))$, the other solving a *dense* linear algebra problem costing $O(\mathsf{T}^{2.4\cdots}(d + r))$.

In the end of their paper [6], B. Barkee *et al.* challenged the researchers to produce sparse cryptographic schemes applying the complexity of Gröbner bases to an ideal membership problem, claiming that they would be even easier to crack, but expressing the will to test their conjecture.

Probably, they were unaware that a sparse scheme of that kind – the so-called *Polly Cracker* - existed from 1992 [26–28]. The key to break such cipher was using a root of the system, which is even simpler than the use of a Gröbner basis.

The public ideal was generated using polynomials coming from combinatorial or algebraic NP-complete problems (hence such systems were naturally named *CA-style* or *California style* cryptographic schemes). Therefore, cryptanalisis was lated based both on satisfiability [39] and on the sparsity of the generators [62–64]. The success of these attacks led researchers to develop totally different cryptosystems, mainly based on binomial ideals/Euclidean lattices [13–16, 2, 3, 46].

For a survey on CA-systems and their analysis see [38].

In 2006, [1] proposed essentially a *verbatim* adaptation of [6]; the main differences are that the Gröbner basis F is taken in a free module over a monoid ring and the public data are the free monoid, the set G (usually a generating set formed by binomials) and the *whole set* $\mathbf{N}(\mathbb{I}(F))$, so that the system is widely open to an oracle attack [4, 11].

However, ten years before, Pritchard [54] published a procedure which is able to crack also the obvious improvement of publishing a subset of terms [12]: the existence, in the non-commutative setting, of infinite Gröbner bases implies that Buchberger Algorithm becomes a semidecision procedure which terminates returning a finite Gröbner basis if and only if such basis is finite; Pritchard adapted such version of Buchberger Algorithm into a semidecision procedure which, given a basis $G \subset Q = \mathbb{F}\langle X_1, \dots, X_n\rangle$ and a polynomial $f \in Q$ terminates if and only if $f \in \mathbb{I}(G)$. It is then a trivial excercise ([50, Figure 47.7]) to adapt Pritchard's Procedure in order to produce an *algorithm* to decrypt any non-commutative version of Barkee's Cryptosystem.

Rai's cryptosystem [56], based on the infiniteness of non-commutative Gröbner bases, and consisting in hiding the (principal) Gröbner basis $\{g\}$ into a public basis $\{l_1 g r_1 \dots l_s g r_s\}$ cannot be cracked via Pritchard's algorithm but yields under Davenport's algorithm factorizing non-commutative polynomials [18].

The proposal by Rai, where the private key is a principal ideal and the public key is a bunch of polynomials within this principal ideal was then recently adapted [12] specializing and extending Stickel's Diffie-Hellman protocols [61, 58, 44, 17] in the setting of Ore extensions $\mathcal{A}$: given public 3 non-commuting elements $L, C, R \in \mathcal{A}$, Alice selects two polynomials $l, r \in \mathbb{F}[X]$ and sends to Bob $l(L)Cr(R)$.

The proposal of [12] has been extended by [20] to (graded) *iterated Ore extensions with power substitutions* $\mathcal{A}$ [53, 49] which, after pointing the potential weakness toward the result by Kandri-Rody–Weispfenning [35] generalized by the Passau school [50, Prop. 49.3.5]), gives an attack through an adaptation of Buchberger reduction.

2 Notation

Given a ring R and a semigroup $(\mathcal{T}, \circ)$ ordered by a semigroup ordering $<$, we consider the R-module $\mathcal{M} := R\langle\mathcal{T}\rangle$ whose generic elements $f \in R\langle\mathcal{T}\rangle \setminus \{0\}$ have a unique representation as an ordered linear combination of terms $t \in \mathcal{T}$ with coefficients in R:

$$f = \sum_{i=1}^{s} c(f, t_i) t_i : c(f, t_i) \in R \setminus \{0\}, t_i \in \mathcal{T}, t_1 > \cdots > t_s.$$

The *support* of f is the set $\mathrm{supp}(f) := \{t : c(f, t) \neq 0\}$; we further denote $\mathbf{T}(f) := t_1$ the *maximal term* of f, $\mathrm{lc}(f) := c(f, t_1)$ its *leading coefficient* and $\mathbf{M}(f) := c(f, t_1) t_1$ its *maximal monomial*.

Here we will consider either

- the commutative ring $\mathcal{P} := \mathbb{F}[X_1, \dots, X_n]$ over a field $\mathbb{F}$, and the semigroup of terms
$$\mathcal{T} := \{X_1^{a_1} \cdots X_n^{a_n} : (a_1, \dots, a_n) \in \mathbb{N}^n\}.$$

- or the free monoid ring $Q := \mathbb{F}\langle\mathbb{Z}\rangle$ over the monoid $\langle\mathbb{Z}\rangle$ of all words over the alphabet $\mathbb{Z}$.
- We will further impose on a submodule of $R[X_1, \dots, X_n]$,

$$\mathcal{A} \cong R[\mathcal{B}] \subset R[X_1, \dots, X_n], \mathcal{B} \subset \mathcal{T}$$

  a twisted ring structure $\mathcal{A} := (R[\mathcal{B}], \star)$ defining on it a multiplication $\star$ which satisfies, for each $f, g \in R[\mathcal{B}]$, $\mathbf{T}(f \star g) = \mathbf{T}(f) \circ \mathbf{T}(g)$

  For any set $F \subset \mathcal{M}$, write

- $\mathbf{T}\{F\} := \{\mathbf{T}(f) : f \in F\}$;
- $\mathbf{M}\{F\} := \{\mathbf{M}(f) : f \in F\}$;
- $\mathbf{T}(F) := \{\tau\mathbf{T}(f) : \tau \in \mathcal{T}, f \in F\} \subset \mathcal{T}$, a semigroup ideal;
- $\mathbf{N}(F) := \mathcal{T} \setminus \mathbf{T}(F)$, an order ideal;
- $\mathbb{I}(F) = \langle F\rangle$ the (in principle two-sided) ideal generated by F.
- $\mathbb{F}[\mathbf{N}(F)] := \mathrm{Span}_{\mathbb{F}}(\mathbf{N}(F))$.

Recall that a generating set F of the ideal $\mathsf{I} := \mathcal{I}(F)$ is called a Gröbner bases if $\mathbf{T}(F) = \mathbf{T}(\mathsf{I})$, that is, $\mathbf{T}\{F\}$ generates $\mathbf{T}(\mathsf{I}) = \mathbf{T}\{\mathsf{I}\}$, and the order ideal $\mathsf{N}(\mathsf{I})$ is called the *Gröbner escalier* of I; moreover for each element $f \in \mathcal{M}$, the unique element

$$g := \mathrm{Can}(f, \mathsf{I}) \in \mathbb{F}[\mathbf{N}(F)]$$

such that $f - g \in \mathsf{I}$ will be called the *canonical form* of f w.r.t. I. It can be computed, if F is Gröbner, via Buchberger reduction.

3 Prologo: an Ur-Barkee Scheme

A scheme which anticipated the Barkee Scheme was developed in 1984, when Wanger and Magyarik proposed [65] to base a public-key cryptosytem on the unsolvability of the word problem. In particular, they proposed to

1. consider
   - a finitely presented group $G := (X, R)$ whose word problem is unsolvable and
   - futher relations[1] S, so that the quotient group $G' := (X, R \cup S)$ has instead a solvable word problem;
   - a finite set of elements $w_1, \dots, w_s \in G$ such that, denoting $\Omega : G \to G'$ the canonical projection, it holds $\Omega(w_i) \not\equiv \Omega(w_j)$ in G', for each pair $i, j, i \neq j$;
2. publish $G := (X, R)$ and $W := \{w_1, \dots, w_s\}$;
3. in order to send the message w_i, one rewrites it using the relations R thus obtaining a word w which is equivalent to w_i in G, so that, in G', $\Omega(\mathsf{w}) \equiv \Omega(w_i)$ and $\Omega(\mathsf{w}) \not\equiv \Omega(w_j)$, $j \neq i$;
4. the receiver then just needs to apply the solvable word problem in G' to decide to which word $\Omega(w_j)$, $\Omega(\mathsf{w})$ is equivalent. □

[1] To be chosen *e.g* in the set

$$\mathcal{A} := X \cup \{x_i x_j^{-1} : x_i, x_j \in X\} \cup \{x_i x_j : x_i, x_j \in X\} \cup \{x_i x_j x_i^{-1} x_j^{-1} : x_i, x_j \in X\}.$$

4 Barkee's cryptosystem

In 1993 B. Barkee *et al.* wrote a paper [6] whose aim was to dispel the urban legend that "Gröbner bases are hard to be computed" [2] and to orient research on applications of Gröbner bases to cryptosystems toward the use of sparse schemes.

To do so, they proposed the most obvious *dense* Gröbner-based cryptosystem remarking that, equally obviously, cracking the system costed *as much as* using it. Their pseudo-system consisted in

1. writing down an easy-to-produce Gröbner basis $F = \{f_1, \ldots, f_s\}$ — this can be efficiently performed via Macaulay's Trick[3] [48] — generating an ideal $\mathsf{I} := \mathbb{I}(F) \subset \mathcal{P}$ and
2. publishing a set $G := \{g_1, \ldots, g_l\} \subset \mathbb{I}(F)$ of *dense* polynomials of degree at most d in $\mathcal{P}$ and a set
$$T := \{\tau_1, \ldots, \tau_s\} \subset \mathbf{N}(\mathbb{I}(F)) = \mathcal{T} \setminus \mathbf{T}(\mathbb{I}(F))$$
of *normal terms* belonging to the Gröbner *éscalier* of $\mathbb{I}(F)$, "either the whole of it, or, for added security, a subset of it" [6];
3. in order to send a message $M := \sum_{i=1}^{s} c_i\tau_i \in \mathrm{Span}_{\mathbb{F}}(T)$, the sender produces random *dense* polynomials $p_j \in \mathcal{P}, 1 \le j \le l, \deg(p_i) = r$ and encrypts M as $C := M + \sum_{j=1}^{l} p_j g_j$;
4. the receiver, possessing the Gröbner basis of $\mathbb{I}(F)$ applies Buchberger's reduction to obtain $\mathrm{Can}(C, \mathbb{I}(F)) = M = \sum_{i=1}^{s} c_i\tau_i$. □

It is easy to realize that denoting, for each $\delta \in \mathbb{N}$,
$$\mathcal{T}_{\le\delta} := \{\tau \in \mathcal{T} : \deg(\tau) \le \delta\} \text{ and } \mathsf{T}(\delta) := \#\mathcal{T}_{\le\delta} = \binom{\delta + n}{n}$$
both encoding and decoding cost between $O(\mathsf{T}(d + r))$ (the time needed to scan a dense message) and $O(\mathsf{T}^2(d+r))$ (the cost of Buchberger's reduction algorithm in the generic case).

The point of the paper was that an enemy would have been able to read the message without even attempting to perform the hard[4] Gröbner basis computation but

[2] which perhaps could be true if, instead of using the most efficient implementations [32,29] of Buchberger's algorithm [7,8] based on Möller Lifting Theorem [47], the decypher applies the obsolete S-polynomial test/completion [9], but is definitely false if Gröbner bases are produced either with Macaulay-like algorithms [40,41] as Faugère's F_4 [24] and F_5 [25] or with involutive algorithms [30,31] based on Janet theory [37].

[3] Given a finite set of terms $m_1, \ldots, m_r \in \mathcal{T}$ let us construct, by repeated GCDs, a finite sequence — a *sequence* and not just a *set* — $M := [n_1, \ldots, n_s] \subset \mathcal{T}$ and subsets $J_i \subset \{1, \ldots, s\}$ $i, 1 \le i \le r$, such that
- for each $i, 1 \le i \le r$, $m_i = \prod_{l \in J_i} n_l$;
- for each $i, j, 1 \le i < j \le r$, $\mathrm{lcm}(m_i, m_j) = \prod_{l \in J_i \cup J_j} n_l$.

Now let us choose, for each $l, 1 \le l \le s$, an element $h_l \in \mathcal{P}$ such that $\mathbf{T}(h_l) < n_l$ and let us define
$\gamma_l := n_l - h_l$, for each $l, 1 \le l \le s$,
$g_i := \prod_{l \in J_i} \gamma_l$, for each $i, 1 \le i \le r$.
Then $G = \{g_i . 1 \le i \le r\}$ is a Gröbner basis such that $\mathbf{T}(G) = (m_1, \ldots, m_r)$.

[4] $O(\mathsf{T}^4_{\le\delta})$ where $\delta := \max(\deg(\tau) : \tau \in \mathbf{G}_<(\mathsf{I}) = O(d^{n2^n})$.

with a more elementary linear-algebra based approach. Namely they proposed two attacks which they labelled as

(A). The Fantomas Attack: consult the library.
(B). The Moriarty Attack: linear algebra.

to which one could add

(C). The Gordan Attack: consult the King of Invariants.

They consist in the following

(A). The Fantomas Attack is based on a result [22] of the TERA community which proved that for a basis $G := \{g_1, \ldots, g_l\}$, $\deg(g_i) \leq d$ and a polynomial C, $\deg(C) \leq d + r$ for which $C - \mathrm{Can}(C, \mathbb{I}(F)) = \sum_{j=1}^{l} p_j g_j$ satisfies $\deg(p_j) \leq r$ it is possible to compute $\mathrm{Can}(C, \mathbb{I}(F))$ by a version of Buchberger's Algorithm modified so that each reduction of S-polynomials of degree higher than $d + r$ is not performed.
The attacker does not know the exact value r since there could be highest-degree cancellation so that $r > \deg(C) - d$ but this is not a problem: computations involving S-polynomials of degree higher then $D := \deg(C)$ are *postponed* instead of being not-performed; if the first round fails, not returning an element in $\mathrm{Span}_{\mathbb{F}}(T)$, the algorithm sets $D := D + 1$ and performs now reductions of S-polynomials of degree bounded by D. Repeating this procedure after $r + d - \deg(C)$ rounds, the attacker finds both r and M.
Being a Buchberger algorithm computation truncated at degree $d+r$, the Fantomas Attack costs $O(\mathsf{T}^4(d + r))$.
(B). The Moriarty Attack consists in simply repeatedly (for $D := \deg(C)..d+r$) solving the dense linear algebra systems with unknowns

$$\left\{b_{j\tau} : \tau \in \mathcal{T}(D - \deg(g_j)), 1 \leq j \leq l\right\} \bigcup \{c_1, \ldots, c_s\}$$

and, as linear equations, the coefficients of each term in $\mathcal{T}$ in the polynomial equation

$$\sum_{\tau \in \mathcal{T}(D)} a_\tau \tau - \sum_{j=1}^{l} \left(\sum_{\tau \in \mathcal{T}(D - \deg(g_j))} b_{j\tau} \tau \right) g_j - \sum_{i=1}^{s} c_i \tau_i = 0$$

where $\sum_{\tau \in \mathcal{T}(D)} a_\tau \tau := C$ is the known received message.
Being a *dense* linear algebra problem, the Moriarty Attack costs $O(\mathsf{T}^3(d+r))$ with Gaussian algebra, $O(\mathsf{T}^{2.4\cdots}(d + r))$ with fast linear algebra.
(C). It consists into a forgetton result by Buchberger [10] who essentially restated Gordan's approach to Hilbert's *Basisisatz* proving that, given a system

$$F = \{g_1, \ldots, g_u\} \subset \mathcal{P} = \mathbb{F}[x_1, \ldots, x_n]$$

of multivariate polynomials, the following three steps yield a Groebner basis for $\mathbb{I}(F)$.
(a) Generate all multiples

$$\mathcal{B} := \{\omega g_i : g_i \in F, \omega \in \mathcal{T}\}$$

Consider the set of these multiples

$$\omega g_i := \sum_{\tau \in \mathcal{T}} c(\omega g_i, \tau)\tau$$

as the rows of an (infinite) Macaulay's Matrix with the columns numbered by the power products $\tau \in \mathcal{T}$ and ordered according to the term ordering w.r.t. to which one wants to find the Groebner basis for F.

(b) Gaussian row-reduce this matrix obtaining a new matrix whose rows give an enumerated set of polynomials $h_i := \sum_{\tau \in \mathcal{T}} c(h_i, \tau)\tau$.

(c) Take the set $G \subset \{h_i, i \in \mathbb{N}\}$ of those polynomials h_i in this triangularized matrix whose leading terms $\mathbf{T}(h_i)$ satisfy

$$\mathbf{T}(h_j) \nmid \mathbf{T}(h_i) \text{ for each } j < i.$$

Of course, this is not an algorithm because the first step is an infinite step that generates an infinite matrix. Therefore, Buchberger posed the question whether one can find an *a priori* bound on the degree D so that, when the above steps are applied to the finite set (and related matrices)

$$\mathcal{B}(D) := \{\omega g_i : g_i \in F, \omega \in \mathcal{T}, \deg(\omega g_i) \leq D\}$$

the returning basis G_D is guaranteed to be Gröbner.
Recently his PhD student Manuela Wiesinger-Widi [66] was able to give such a bound with a relatively easy proof using a combination of Hermann's bound [34] and the bound given by Dubé [23]. Her degree bound is as follows

Theorem 41 (Wiesinger-Widi) *[66] Let n be the number of variables, u be the number of polynomials in F, and $d := \max(\deg(f), f \in F)$, $\mathsf{I} = \mathbb{I}(F)$.
Then, in the above procedure, it suffices to take $\mathcal{B}(D)$ with*

$$D = 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}} + \sum_{j=0}^{n-1} (ud)^{2^j}$$

*in order to obtain the required Gröbner basis G_D.
If the above procedure is applied to $\mathcal{B}(D_0)$ with*

$$D_0 = \sum_{j=0}^{n-1} (ud)^{2^j}$$

then $\mathcal{Z}(\mathsf{I}) = \emptyset \iff 1 \in \mathbf{T}(G_{D_0})$.

Remark 42 *Of course this bound is definitely outside the theme of Barkee's approch, but we consider important to point this precise bound, which by choice does not consider coefficient explosion, to the community applying polynomials with coefficient in finite fields.*

5 Intermezzo: Polly Cracker

B. Barkee *et al.* concluded their paper [6] with a challange:

> A cryptographic scheme applying the complexity of Gröbner bases to an ideal membership problem is bound to fail. Is our reader able to find a scheme which overcomes this difficulty? In particular our reader could think (perhaps with some reason) that a *sparse* scheme could work. We believe (perhaps without reason) that sparsity will make the scheme easier to crack. We would be glad to test our belief on specific sparse schemes.

Boo was unaware that a *sparse* cryptographic scheme based on the ideal membership problem was already developed by Fellows and Kobitz [26–28] in 1992, under the label of *Polly Cracker*, where the trapdoor of their system is not a Gröbner basis of the ideal, but, more simply, a root of it. What is more important, the polynomials generating the public ideal are derived from combinatorial or algebraic NP-complete problems (hence such systems were naturally named CA-systems). This oriented to consider both analysis based on satisfiability [39] and attacks exploiting the sparsity of the generators [62–64]. Soon the research oriented toward cryptosystems based on binomial ideals/Euclidean lattices [13–16, 2, 3, 46].

But this is another story to which Boo did not contribute. For a survey on CA-systems and their analysis see [38].

6 Noncommuatative Gröbner bases

6.1 A non-commutative version of Barkee's Cryptosystem

Having thus disposed of the urban legend that "Gröbner bases are hard to be computed", we need now to dispel another urban legend that "non-commutative Gröbner bases are impossible to be computed being infinite". Before doing that, we simply cryptanalize the proposal of [1], which is essentially a *verbatim* adaptation of [6]; the main differences are:

1. the Gröbner basis F is taken in a free module over a monoid ring, a Gröbner basis theory and a Buchberger's Algorithm in this setting being proposed in [42, 57].
2. the public data are the free monoid, the set G, usually made of binomials, and the *whole set* $\mathbf{N}(\mathbb{I}(F))$;

moreover sparsity/density of the data is not discussed.

The omission of the crucial *caveat* of [6] "*for added security, a subset*" of $\mathbf{N}(\mathbb{I}(F))$ led them to publish the whole set $\mathbf{N}(\mathbb{I}(F))$ and, consequently, to make known the set $\mathbf{T}(G) = (m_1, \dots, m_r)$. This choice left them *no defence* against

(E). The Bulygin Attack: chosen ciphertext attack.
Bulygin [11], in his attack, remarks that, for each $f_i \in F$, it holds $\mathrm{Can}\left(\mathbf{T}(f_i), \mathbb{I}(F)\right) = f_i - \mathbf{T}(f_i)$. He thus built fake ciphertexts

$$\tilde{C}_i := \sum_{j=1}^{\ell} p_j g_j + \mathbf{T}(f_i).$$

The decrypted version of this message being $\mathrm{Can}\,(\tilde{C}_i, \mathbb{I}(F)) = f_i - \mathbf{T}(f_i)$, allows then to obtain the polynomials $f_i = \mathrm{Can}\,(\tilde{C}_i, \mathbb{I}(F)) + \mathbf{T}(f_i)$ of the secret key.

6.2 Rai: Protecting Barkee's scheme against Bulygin's Attack

Rai [56] remarked that it is not difficult to detect the fake ciphertexts $\tilde{C}_i$ just specializing the vague statement of [6] *public [. . .] , for added security, a subset* $T := \{\tau_1, \ldots, \tau_s\} \subset \mathbf{N}(\mathbb{I}(F))$ of [6] in order to make step 2 of Section 4 solid against Attack 6.1.

He in fact suggests to publish a subset $T \subset \mathbf{N}(\mathbb{I}(F))$ such that :

$$(\mathbf{N}(\mathbb{I}(F)) \setminus T) \cap \mathrm{supp}(f_i) \neq \emptyset, \forall i, 1 \leq i \leq s.$$

The decryption procedure will be then modified so that an error message is returned as soon as the decrypted message M does not satisfy $\mathrm{supp}(M) \subset T$.

6.3 Finite computation of non-commutative Gröbner Bases

The claimed security, however, of Rai's variation [55] is based on the fake urban legend on the uncomputability of non-commutative Gröbner bases due to their infinite size. While it is true that such bases are infinite it is equally true that some infinite Gröbner bases can be produced (and their property proved) with a few and easy hand computation; for instance [33, p.99] proves that

Proposition 61 *Under the degree-lexicographical ordering induced by* $x < y$ *the principal ideal* $\mathbb{I}(p_0) \subset \mathbb{F}\langle x, y\rangle, p_0 = yxy - xyx$ *has, as a Gröbner basis, the infinite basis* $G = \{p_i, i \in \mathbb{N}\}$ *where we define* $p_i := yx^{i+1}yx - xyxxy^i$.

Moreover, Ufnarovski's implementation in the system BERGMAN [5] is able to compute those infinite Gröbner bases representing *finite state automata* [21] while it is not sufficent to prove their being Gröbner. An analysis [45, p.35] of all homogeneus pure binomials in $\mathbb{F}\langle x, y\rangle$ of degree bounded by 6,

deg.	fin.	inf. reg.	not reg.	#
2	4	2	0	6
3	18	8	2	28
4	65	39	16	120
5	271	176	49	496
6	1019	845	152	2016

shows that most either have a finite Gröbner basis or an infinite regular bases computable via Ufnarovski approach and that only nearly 10% of these ideals have an infinite but not regular Gröbner basis.

6.4 Pritchard's Decryption Algorithm

Generalizing Buchberger Theory of Gröbner bases to non-commutative settings is simple, but lacking a generalization of Noetherianity, they may be infinite. The existence of such infinite bases modifies the status of a Buchberger Algorithm for producing them, making it a semidecision procedure which terminates returning a finite Gröbner basis if and only if such basis is finite.

Actually, Pritchard [54], reformulating in this setting the original approach of [22], adapted such version of Buchberger's algoritm to a semidecision procedure which, given a basis $G \subset Q := \mathbb{F}\langle X_1, \dots, X_n\rangle$ and a polynomial $f \in Q$ terminates if and only if $f \in \mathbb{I}(G)$.

Given a polynomial $f \in Q$ and a countable[5] sequence

$$F := \{f_i, i \geq 1\} \subset Q, f_i = \mathbf{M}(f_i) - p_i =: c_i\tau_i - p_i,$$

and considered the twosided ideal $\mathsf{M} := \mathbb{I}(F)$, Pritchard's procedure, once fixed a sequential[6] term ordering $\prec$ and enumerated a sequence of elements

$$\upsilon_1, \upsilon_2, \dots, \upsilon_i, \upsilon_{i+1}, \dots$$

such that $\upsilon_i \prec \upsilon_{i+1}$ for each i iteratively computes a sequence of finite sets

$$G_i = \left\{g_1^{(i)}, \dots, g_{s(i)}^{(i)}\right\} \subset \mathsf{M} \setminus \{0\}, i \geq 1$$

which satisfy the following properties

1. $G_1 \subseteq G_2 \subseteq \cdots \subseteq G_i \subseteq \cdots \subseteq \mathsf{M}$;
2. for each $j \leq i$, there is $\ell(j) \leq s(i)$ such that $f_j = g_{\ell(j)}^{(i)} \in G_i$;
3. for each i and each member of the syzygy basis for G_{i-1} truncated at υ_{i-1}

$$B_i := \left\{\sum_{k=1}^{\mu} d_k\lambda_k e_{l_k}\rho_k, \text{ for each } k, \lambda_k\tau_k\rho_k \prec \upsilon_{i-1}\right\}$$

   the S-polynomial $\sum_{k=1}^{\mu} d_k\lambda_k g_{l_k}^{(i-1)}\rho_k \in \mathbb{I}_2(G_{i-1}) \subset \mathsf{M}$ has a bilateral Gröbner representation in terms of G_i

each G_i and $\ell(i)$ being defined as

$$G_i := G_{i-1} \cup \{f_i\} \cup \{NF(g, G_{i-1} : g \in B_i\} \setminus \{0\} \text{ and } \ell(i); = \#G_{i-1} + 1.$$

At each iterative loop, one performs a (further step of) Buchberger reduction of f w.r.t. G_i, the procedure continues unless $NF(f, G_i) = 0$ for some i, proving that $g \in \mathsf{M}$.

[5] If the sequence is finite $F := \{f_i, u \geq i \geq 1\}$ we can simply set, for each $i > u$ either $f_i := 0$ or $f_i := f_u$.

[6] *id est* a term ordering $\prec$ on $\mathcal{T}^m$ is called *sequential* if for each $\tau \in \langle X_1, \dots, X_n\rangle^m$ the set $\{\omega \in \langle X_1, \dots, X_n\rangle : \omega \prec \tau\}^m$ is finite.

Remark 62 *It is clear that, if at each step we denote by τ_i any term such that each member $\sum_{k=1}^{\mu} d_k\lambda_k e_{l_k}\rho_k$ of the syzygy basis for G_{i-1} satisfies, for each k, $\lambda_k\tau_k\rho_k \prec \upsilon_i$, then the procedure terminates if and only if $G_i = G_{i-1}$; this happens if and only if* M *has a finite Gröbner basis, in which case the procedure returns $G_i = G_{i-1}$ as such finite Gröbner basis.*

More easily, it is a trivial task to modify Pritchard's procedure so that, given a basis $G \subset Q$, a polynomial $C \in Q$ and a finite set of terms

$$T \subset \mathbf{N}(\mathbb{I}(F)) \subset \langle X_1, \dots, X_n \rangle,$$

terminates if and only if $M := \mathrm{Can}(C, \mathbb{I}(G)) \subset \mathrm{Span}_{\mathbb{F}}(T)$, in which case it returns such a canonical form, thus reading the message $M := \mathrm{Can}(C, \mathbb{I}(F))$ encrypted as C.

6.5 Rai's cryptosystem and non-commutative polynomial

Rai's cryptosystem [55], based on the infiniteness of non-commutative Gröbner bases, and consisting in hiding the (principal) Gröbner basis $\{g\}$ into a public basis $\{l_1 g r_1, \dots, l_s g r_s\}$ cannot be cracked via Pritchard's algorithms but yields under Davenport's algorithm factorizing non-commutative polynomials [18].

7 Why you should not even think to use Ore algebras in Cryptography

7.1 Burger–Heinle Diffie-Hellman-like scheme

In 2014 Burger–Heinle [12] reproposed essentially Ray's application of principal ideals this time as a Diffie-Hellman-like scheme; the chose as their setting not the non-commutative free algebras but a multivariate Ore extension [52,19] S, attributing the strength of their proposal to the hardness of factorizing in R.

In their proposal, the two communicating parties, Alice and Bob, choose a multivariate Ore extension S with constant subring R and agree on non-central elements $L, P, Q \in S$, non-mutually commuting; all these data are public. Alice picks secretly a pair of commuting polynomials $(P_A, Q_A) \in R[X] \times R[X]$ and Bob chooses another pair of the same fashion $(P_B, Q_B) \in R[X] \times R[X]$. Finally, Alice sends Bob $A = P_A(P)LQ_A(Q)$ and receives $B = P_B(P)LQ_B(Q)$ from him. Note that both pairs $P_A(P), P_B(P)$ and $Q_A(P), Q_B(P)$ commute while there is no commutation be between the elements $P_*(P)$ and $Q_*(P)$, since neither P nor Q commute with L. Thus the shared secret is given by

$$P_A(P)BQ_A(Q) = P_A(P)P_B(P)LQ_B(Q)Q_A(Q) = P_B(P)P_A(P)LQ_A(P)Q_B(P) = P_B(P)AQ_B(Q).$$

7.2 And its generalization

Instead of cryptoanalizing Burger–Heinle scheme we intend to consider the widest similar setting, namely *iterated Ore extensions with power substitutions* $\mathcal{A}$ [49,**?**].

Definition 71 *Let us denote by $\circ$ the commutative multiplication of $\mathcal{T}$ and $<$ a term ordering on it. A left module over an effective ring R*

$$\mathcal{A} \cong R[\mathcal{B}] \subset R[X_1, \ldots, X_n], \mathcal{B} \subset \mathcal{T}$$

endowed with a multiplication $\star$ which satisfies

1. *for each term $\tau \in \mathcal{B} \subset \mathcal{T}$ there are an automorphism $\alpha_\tau : R \to R$ and an α_τ-derivation $\theta_\tau : R \to R$ so that for each $r \in R$, $t \star r = \alpha_t(r)t + \theta_t(r)$;*
2. *for two terms $\tau_1, \tau_2 \in \mathcal{B} \subset \mathcal{T}$, there are elements $\varpi(\tau_2, \tau_1) \in R$ and $\Delta(\tau_2, \tau_1) \in \mathcal{A}, \mathbf{T}(\Delta(\tau_2, \tau_1)) < \tau_2 \circ \tau_1$ such that $\tau_2 \star \tau_1 = \varpi(\tau_2, \tau_1)\tau_2 \circ \tau_1 + \Delta(\tau_2, \tau_1)$.*
3. *$c_u\tau_u \star c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\tau_u \circ \tau_v + h, h \in \mathcal{A}, \mathbf{T}(h) < \tau_u \circ \tau_v$*

is defined an iterated Ore extensions with power substitutions

Example 1 Let $\mathcal{A} = \mathcal{R}[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ with the arithmetics

$$X_j \star X_i = a_{ij}X_iX_j, \quad Y_l \star X_j = b_{jl}X_j^{e_i-1}(X_jY_l), Y_k \star Y_l = c_{lk}Y_lY_k$$

where a_{ij}, b_{jl}, c_{lk} are invertible elements in $\mathcal{R}$, $e_i \in \mathbb{N}^*$. Thus

(a). $c_u\tau_u \star c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\tau_u \circ \tau_v$.
(b). $\alpha_{\tau_u} = \mathrm{Id}, \theta_\tau = 0, \Delta(\tau_2, \tau_1) = 0$ for each $\tau_u, \tau_2, \tau_1 \in \mathcal{B}$.
(c). $\tau_u \circ \tau_v = \Upsilon(\tau_u, \tau_v)\tau_u\tau_v, \Upsilon(\tau_u, \tau_v) \in \{X_1^{d_1} \cdots X_n^{d_n} \mid (d_1, \ldots, d_n) \in \mathbb{N}^n\}$;
(d). $c_u\tau_u \star c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\Upsilon(\tau_u, \tau_v)\tau_u\tau_v = \varpi(\tau_u, \tau_v)\Upsilon(\tau_u, \tau_v) \cdot c_u\tau_u \cdot c_v\tau_v$.

7.3 The Passau Attack

We point out that, as for noncommutative cryptosystems an attack was already known [54], also in this case, a potential attack is present and can be deduced by the result introduced by Kandri-Rody–Weispfenning result [35][50, IV.Prop.49.3.5] and constantly extended in all the results of the Passau school and which is a direct consequence of condition of Definition 71.3.

Proposition 72 *For each $f, g \in \mathcal{A}$ there are $d \in R \setminus \{0\}, h \in \mathcal{A}, \mathbf{T}(h) < \mathbf{T}(f)\mathbf{T}(g)$ such that*

$$f \star g = d \cdot f \cdot g + h.$$

We do not care to discusse whether and how the Passau Attack could crash such Diffie-Hellman protocol in our setting since we are able to recover the common key by the simple application of Buchberger Reductiom.

7.4 Stickel's Key Exchange Protocol

Before proposing our attack (Section 7.5), we intend to introduce a survey on protocols similar to the one proposed in [12] and extended here.

- In Stickel's proposal [61] Alice and Bob, choose a non-abelian finite group G and agree on two elements $P, Q \in G, PQ \neq QP$; all these data are public. Alice picks secretly a pair of integers (P_A, Q_A) and Bob chooses another pair of the same fashion (P_B, Q_B). Alice sends Bob $A = P^{P_A}Q^{Q_A}$ and receives $B = P^{P_B}Q^{Q_B}$ from him. Thus the shared secret is given by

$$P^{P_A}BQ^{Q_A} = P^{P_A+P_B}Q^{Q_A+Q_B}Q_A(Q) = P^{P_B}AQ^{Q_B}.$$

  He proposed to use $G := GL_n(\mathbb{F}_n)$. Some weaknesses of the scheme are discussed in [60, ?]. [58] considers more secure working on the set $M_n(R)$ of all metrices of order n over a finite ring R.
- Shpilrain [58] also proposed, 6 years before, a variation of the scheme as [12]. Alice and Bob, choose a finite ring R and agree on two elements $P, Q \in M_n(R), PQ \neq QP$; all these data are public. Alice picks secretly a pair of commuting polynomials $(P_A, Q_A) \in R[X] \times R[X]$ and Bob chooses another pair of the same fashion $(P_B, Q_B) \in R[X] \times R[X]$. Finally, Alice sends Bob $A = P_A(P)Q_A(Q)$ and receives $B = P_B(P)Q_B(Q)$ from him, the shared secret being

$$P_A(P)BQ_A(Q) = P_A(P)P_B(P)Q_B(Q)Q_A(Q) = P_B(P)P_A(P)Q_A(P)Q_B(P) = P_B(P)AQ_B(Q).$$

  Mullan [51] successfully mounted a linear algebra attack on it
- Another variation was proposed in 2007 in [44] (see also [43, 59]). Alice and Bob, choose a finite semiring R with nonempty center C, not embeddable into a field and agree on three elements $C, P, Q \in M_n(R)$; all these data are public. Alice picks secretly a pair of commuting polynomials $(P_A, Q_A) \in C[X] \times C[X]$ and Bob chooses another pair of the same fashion $(P_B, Q_B) \in C[X] \times R[X]$. Alice sends Bob $A = P_A(P)CQ_A(Q)$ and receives $B = P_B(P)CQ_B(Q)$ from him, the shared secret being

$$P_A(P)BQ_A(Q) = P_A(P)P_B(P)CQ_B(Q)Q_A(Q) = P_B(P)P_A(P)CQ_A(P)Q_B(P) = P_B(P)AQ_B(Q).$$

- In the same year [17] proposes a Diffie-Hellman-like protocol which evaluates univariate polynomials over elements and agreed non-commutative ring R. Alice picks $a, b \in R, m, n \in \mathbb{N}, f \in \mathbb{Z}[X]$ and sends Bob $m, n, a, b, A := f(a)^m bf(a)^n$; Bob chooses $h \in \mathbb{Z}[X]$ and sends Alice $A := h(a)^m bh(a)^n$ the shared secret being

$$f(a)^m Bf(a)^n = f(a)^m h(a)^m bh(a)^n f(a)^n = h(a)^m Ah(a)^n.$$

- Finally, simplifying [17], [36] proposes verbatim the suggestions of both [44] and [12] in the most general setting: an agreed non commutative ring R whose center is denoted $Z(R)$, three agreed elements, $P, Q \in R, C \in R \setminus Z(R)$, the four polynomials being selected in $Z(R)[X]$.

7.5 A Buchberger-like Attack

Suppose the polynomials $P, Q, L \in \mathcal{A}$ (P, Q non commuting with L) to be *publicly known*, whereas the polynomials $f, g \in R[t]$ are *kept secret*. Since Alice sends $A := f(P)Lg(Q)$, an eavesdropper can get it, with the aim of discovering f, g.

The polynomial g has the form $g(t) = \sum_{i=a}^{d} c_i t^i$, $a \leq d$, $c_a \neq 0$, so that $g(Q) = \sum_{i=a}^{d} c_i Q^i$. Given a term ordering on $\mathcal{A}$, we can deduce the leading term $\mathbf{T}(\mathbf{Q})$ of Q and the tail of Q (denoted by $tail(Q)$). We define a new variable B and we reduce A from the right using the following rewriting rule:

$$\mathbf{T}(\mathbf{Q}) \to \mathrm{tail}(\mathbf{Q}) + \mathbf{B}.$$

After $a + 1$ reduction steps one gets

$$f(P)L \sum_{i=a}^{d} c_i Q^i \to f(P)L \sum_{i=a+1}^{d} c_i Q^{i-a-1} B \cdot B^a + f(P)Lc_a B^a =$$

$$= XB \cdot B^a + YB^a$$

In this case, $Y := f(P)Lc_a$ and $X := f(P)L \sum_{i=a+1}^{d} c_i Q^{i-a-1}$, so:

- dividing Y by L from the right it is possible to find $f(P)$ and f can be retrieved by reducing w.r.t. P;
- dividing X by Y from the left we get $L \sum_{i=a+1}^{d} c_i Q^{i-a-1}$

the only remaining problem is: how to be sure to have reached the case $Y := f(P)Lc_a$ and $X := f(P)L \sum_{i=a+1}^{d} c_i Q^{i-a-1}$, being a unknown?
To understand this, we evaluate whether $Y \mid_L X$. If so, we got to the case, otherwise we reduce from the right until the answer becomes "Yes".
We conclude by remarking that, by symmetry, we can find $Lg(Q)$ and f.

8 Continue?

References

1. P. Ackermann, M. Kreuzer Gröbner basis cyptosystems *J. Appl. Alg.* **17** (2006) 173–194
2. M.R. Albrecht, P. Farshim, J.-C. Faugère, L. Perret *Polly Cracker, Revisited* L.N.C.S **7073**, pp. 179-196 (2011)
3. M.R. Albrecht, P. Farshim, J.-C. Faugère, L. Perret *Polly Cracker, Revisited* Designs, Codes and Cryptography **79** (2016) 261–302
4. M.E. Alonso, M.G. Marinari, T. Mora *"Oracle-Supported Drawing of the Gröbner éscalier"*. preprint (2008).
5. Backelin J., Cojocaru S., Ufnarovski V. Mathematical Computations using Bergman Lund University
6. B. Barkee, D.C. Can, J. Ecks, T. Moriarty, R.F. Ree. Why you cannot even hope to use Gröbner Bases in Public Key Cryptography. *J. Symb.Comp.* **18** (1994), 497–501.
7. B. Buchberger (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph. D. Thesis, Innsbruck.
8. B. Buchberger (1970). Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischunssystem. *Aeq. Math.* **4**, 374–383.
9. B. Buchberger, *A Criterion for Detecting Unnecessary Reduction in the Construction of Gröbner bases* L.N.C.S **72**, pp. 3–21 (1979).
10. B. Buchberger, *Miscellaneours Results on Groebner Bases for Polynomial Ideals II.* Technical Report 83/1, University of Delaware, Department of Computer and Information Sciences, 1983. p. 31.
11. Bulygin S. *Chosen-cyphertext attack on noncommutative Polly Cracker* Availabe at `https://arxiv.org/abs/cs/0508015`
12. R. Burger, A. Heinle. *A Diffie-Hellman-like key exchange protocol based on multivariate Ore polynomials.* preprint (2014). Availabe at `https://arxiv.org/pdf/1407.1270.pdf`

13. M. Caboara, F. Caruso, C. Traverso *Gröbner Bases for Public Key Cryptography*. To appear on ACM Press, NewYork, ISSAC 08: Proceedings of the 2008 International Symposium on Symbolic and Algebraic Computation.
14. M. Caboara, F. Caruso, C. Traverso *Block lattice polly cracker, theory and practice*. Second Workshop on Mathematical Cryptology, Santander, 24-27 Ottobre 2008. pp. 75–82. [Extended Abstract]
15. M. Caboara, F. Caruso, C. Traverso *Heterogeneous lattice metrics and the NTWO cryptosystem* Second Workshop on Mathematical Cryptology , Santander, 24-27 Ottobre 2008. pp. 118–121.
16. M. Caboara, F. Caruso, C. Traverso *Block Lattice Polly Cracker: design, implementation and security* J. Symb. Comput. 46(5): 534-549 (2011)
17. Cao, Z., Dong, X. and Wang, L.: New Public Key Cryptosystems using polynomials over Non-commutative rings, Cryptology e-print Archive, 2007. Availabe at `https://eprint.iacr.org/2007/009.pdf`
18. F. Caruso *Factorization of Non-Commutative Polynomials* Availabe at `https://arxiv.org/abs/1002.3180` (2010)
19. Ceria, M., Mora, T., *Buchberger-Zacharias Theory of Multivariate Ore Extensions*, Journal of Pure and Applied Algebra Volume 221, Issue 12, December 2017, Pages 2974-3026
20. M. Ceria, T. Moriarty, A. Visconti, *Why you should not even think to use Ore algebras in Cryptography* Availabe at `https://www.researchgate.net/publication/335608455_Why_you_should_not_even_think_to_use_Ore_algebras_in_Cryptography`
21. Cojocaru S., Ufnarovski V., *Noncommuatative Gröbner basis, Hilbert series, Anick's resolution and BERGMAN under MS-DOS*, Computer Science Journal of Moldova **3** (1995), 24–39
22. A. Dickenstein, N. Fitchas, M. Giusti, C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in single exponential time*, Discrete Applied Mathematics **33** (1991) 73–94
23. ,T.W. Dubé, *The Structure of Polynomial Ideals and Gröbner Bases* SIAM J. Comput., **19**(4) (2006)
24. J.-C. Faugère, *A new efficient algorithm for computating Gröbner bases (F_4)*, J. Pure Appl. Algebra **139** (1999), 61–88
25. J.-C. Faugère, *A new efficient algorithm for computating Gröbner bases without reduction to zero (F_5)*, Proc. ISSAC 2002 (2002), 75–83, ACM
26. M.R. Fellows, N. Koblitz, Kid krypto. Advances in Cryptography – Crypto'92,*Lect. N. Comp. Sci.* **740** (1993) 371–389
27. M.R. Fellows, N. Koblitz, Combinatorially based cryptography for children (and adults). *Congressus Numerantium* **99** (1994) 9–41
28. M.R. Fellows, N. Koblitz, Combinatorial cryptosystems galore! *Contemporary Math.* **168** 51–61 (1994)
29. R. Gebauer and H.M. Möller, *On an Installation of Buchbgerger's Algorithm*. J. Symb. Comp. **6**, 275–286 (1988).
30. V.P. Gerdt and Y.A. Blinkov, *Involutive bases of Polynomial Ideals*, Math. Comp. Simul. **45** (1998), 543–560
31. V.P. Gerdt and Y.A. Blinkov *Minimal involutive bases*, Math. Comp. Simul. **45** (1998), 519–541
32. A. Giovini A. *et al.*, *"One sugar cube, please" OR Selection strategies in the Buchberger algorithm*, Proc. ISSAC '91 (1991), 49–54, ACM
33. Green E.L., Mora T., Ufnarovski V. *The Non-Commutative Gröbner Freaks Progress in Computer Science and Applied Logic* **15** (1991), 93–104, Birkhäuser
34. Hermann G., *Die Frage der endlich vielen Schritte in die Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788
35. Kandri-Rody, A., Weispfenning, W., *Non-commutative Gröbner Bases in Algebras of Solvable Type*, J. Symb. Comp. **9** (1990), 1–26
36. Shamsa Kanwal, Saba Inam, Rashid Ali, Shuming Qiu Two New Variants of Stickel's Key Exchange Protocol Based on Polynomials over Noncommutative Rings
37. M. Janet, *Sur les systèmes d'équations aux dérivées partielles* J. Math. Pure et Appl., **3** (1920), 65–151
38. F. Levy-dit-Vehel, M.G. Marinari, L. Perret, C. Traverso, *A Survey on Polly Cracker Systems* in M. Sala et al. (Ed.) *Gröbner bases, Coding, Cryptography*, Springer Risc XVI, (2009) 285–305
39. F. Levy-dit-Vehel, L. Perret *A Polly Cracker System Based on Satisfiability* Progress in Computer Science and Applied Logic **23** (2004) 177–192
40. F.S. Macaulay, *On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers*, Math. Ann. **74** (1913), 66–121
41. F.S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press (1916)
42. K. Madlener, B. Reinert, *Computing Gröbner bases in monoid and group rings*, Proc.ISSAC '93, ACM (1993), 254–263

43. G.Maza Algebraic Methods for Constructing One-Way Trapdoor Functions, PhD Thesis, University of Notre Dame, 2003 Availabe at `http://user.math.uzh.ch/maze/Articles/DissJoli.pdf`
44. G.Maza, C. Monico and J. Rosentha Public Key Cryptography based on Semigroup Actions [pdf arXiv]. In Advances of Mathematics of Communications, Vol. 1, 4 (2007), pp. 489-507 Availabe at `https://www.math.uzh.ch/aa/fileadmin/user/rosen/publikation/ma07.pdf`
45. K. Mårtensson, *An Algirithm to Detect Regular Behaviour of Binomial Gröbner Basis Rational Language*, Master's Thesis, Lund University (2006)
46. D. Micciancio, C. Peikert *Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller* L.N.C.S **7237**, pp. 700-718 (2010).
47. H.M. Möller, *On the construction of Gröbner bases using syzygies*, J. Symb. Comp. **6** (1988), 345–359
48. F. Mora. De Nugis Groebnerialium 2: Applying Macaulay's Trick in order to easily write a Groebner basis *J. Appl. Alg.* (2003)
49. B. Nguefack, E. Pola, *Effective Buchberger-Zacharias-Weispfenning theory of skew polynomial extensions of restricted bilateral coherent rings*, J. Symb. Comp. (2019), Doi:https://doi.org.10.1016/j.jsc.2019.03.003
50. T. Mora, *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016)
51. Mullan, C.: Some results in group-based cryptography, Technical report, Department of Mathematics, Royal Holloway, University of London, (2012).
52. Ore O., *Theory of non-commutative polynomials* , Ann. Math. **34** (1933), 480–508
53. Pesch M., *Gröbner Bases in Skew Polynomial Rings* Dissertation,Passau (1997)
54. Pritchard F. L., *The ideal membership problem in non-commutative polynomial rings*, J. Symb. Comp. **22** (1996), 27–48
55. T.S. Rai *Infinite Gröbner bases and Noncommutative Polly Cracker Cryptosystems* PhD Thesis, Virginia Polytechnique Institute and State Univ. (2004)
56. T.S. Rai *Countering chosen-ciphertext attacks against noncommutative polly cracker cryptosystems* (2005) Cryptology ePrint Archive: Report 2005/344 `https://eprint.iacr.org/2005/344.pdf`
57. Reinert B., *On Gröbner Bases in Monoid and Group Rings*, Thesis, Kaiserslautern (1995)
58. Shpilrain,V.: Cryptanalysis of Stickel's key exchange scheme, Proceedings of Computer Science in Russia,5010,283-288,(2008)
59. V.Shpilrain and A.Ushakov. Thompson's group and public key cryptography. In Third International Conference, ACNS 2005, volume 3531 of Lecture Notes in Comput. Sci., pages 151-163. Springer, Berlin, 2005. Availabe at `https://arxiv.org/pdf/math/0505487v1.pdf`
60. Sramka, Michal. (2008). On the Security of Stickel's Key Exchange Scheme. JCMCC. The Journal of Combinatorial Mathematics and Combinatorial Computing. 66.
61. Stickel,E.: A new method for exchanging secret key, Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), 426-430, Sidney, Australia, (2005)
62. R. Steinwandt, W. Geiselmann, R. Endsuleit *Attacking a polynomial-based cryptosystem: Polly Cracker.* Int. J. Inf. Secur. **1** (2002) 143–148.
63. R. Steinwandt, W. Geiselmann, *Cryptoasnalysis of Polly Cracker.* IEEE Trans. Inf. Th. **48**(11) (2002) 2990–1.
64. D. Hofheinz, R. Steinwandt *A "Differential" Attack on Polly Cracker.* Int. J. Inf. Secur. **1** (2002) 143–148.
65. N.R. Wagner, M.R. Magyarik *A Publyc-Key Cryptosystem based on the Word Problem.* L. N. Comp. Sci **196** (1985), 19-36, Springer
66. M. Wiesinger-Widi Groebner Bases and Generalized Sylvester Matrices. Ph.D. Thesis, Johannes Kepler University, Institute for Symbolic Computation, submitted 2014. Availabe at `https://www.dk-compmath.jku.at/publications/phd-theses/2015-06-05/view`