Noncommutative Polly Cracker-type cryptosystems and chosen-ciphertext security

Tapan Rai * and Stanislav Bulygin †

December 4, 2008

Abstract

In this paper we consider chosen-ciphertext attacks against noncommutative Polly Cracker-type cryptosystems. We present several versions of these attacks, as well as techniques to counter them. First we introduce a chosen-ciphertext attack, which assumes a very simple private key. We then present generalizations of this attack which are valid in more general situations, and propose a simple but effective technique to counter these attacks. Finally, we show how this technique can also be used to counter the adaptive chosen- ciphertext attacks against noncommutative Polly Cracker-type cryptosystems.

Keywords: Chosen-ciphertext attacks, noncommutative Polly Cracker cryptosystems, polynomial-based cryptography, security, Gröbner basis cryptosystems.
2000 Mathematics Subject Classification: Polynomial ideals, Gröbner bases 13P10; Cryptography 94A60.

1 Introduction

This paper presents some applications of Gröbner bases in public-key cryptography. The Algorithmic theory of Gröbner bases was developed by Bruno

*School of Engineering and Mathematics, Edith Cowan University, Joondalup, Western Australia, Australia, t.rai@ecu.edu.au, www.tapan.info

†Department of Mathematics, University of Kaiserslautern,P.O. Box 3049, 67653 Kaiserslautern, Germany, bulygin@mathematik.uni-kl.de, www.mathematik.uni-kl.de/~bulygin/

Buchberger ([4]) for the commutative case and later for the noncommutative case by Teo Mora ([18]). The cryptosystem we are about to consider is the Polly Cracker public-key cryptosystem. Since it was first proposed by [9], a number of authors have studied the Polly Cracker cryptosystem, which has its security based on the intractability of the ideal membership problem for a polynomial algebra over a finite field. Most of these works, (see [8], [10], [12], and [22]) have focused on various attacks against the Polly Cracker cryptosystem. Only a few papers, such as [16], [15], [14] have attempted to develop secure systems based on the ideal membership problem. The authors are aware of the fact that the Polly Cracker cryptosystem is not widely supported in the cryptographic community. Nevertheless, it is also true that the full potential of some concept may be out of reach at the moment and more intensive study is needed to reveal it. This paper is trying to move further on the way of understanding the Polly Cracker better, so that we might better comprehend its weaknesses and thus giving more tools to overcome them.

The noncommutative variant of the Polly Cracker cryptosystem was first proposed by [21] and has been studied by [1]. In this article we extend the results of [10] and [22] in presenting a chosen-ciphertext attack against certain instances of noncommutative Polly Cracker-type cryptosystems (initially in [5]). We then present generalized versions of this attack, which can be used against virtually all Polly Cracker-type cryptosystems. Afterwards we propose a simple but effective technique to counter these attacks. We also consider adaptive chosen-ciphertext attacks which were proposed in [7] and [20]. We specifically consider an adaptive chosen-ciphertext attack against Polly Cracker cryptosystems, which is described by [13], and present a technique to counter it. It should be mentioned that chosen-ciphertext attacks on public-key cryptosystems can be prevented using supplementary techniques like hash functions. Good examples here are Optimal Asymmetric Encryption Padding (OAEP), [3], and Rapid Enhanced-security Asymmetric Encryption Transform (REACT), [19]. But it is definitely of interest to provide protective mechanisms within the cryptosystem itself without the use of these supplementary techniques. This paper elaborates on the latter.

2 Preliminaries

There are several good references to public-key cryptography, for example see [17] and [13]. Rather than re-hash this well- established concept, we

will concentrate on the some background information on Polly Cracker-type cryptosystems.

[9] proposed a class of combinatorial-algebraic cryptosystems, in which they showed how to use computationally hard combinatorial problems to find trap-door functions that serve as the source of public keys. The generalized version of this class of cryptosystems, which has its security based on the intractability of the ideal membership problem for a commutative algebra over a finite field, is called the *Polly Cracker* cryptosystem. We present the generic version of the (commutative) Polly Cracker cryptosystem below:

Let K be a finite field, and X a finite set of variables. Let I be an ideal in $K[X]$ and suppose $G = \{g_1, g_2, \ldots, g_t\}$ is a Gröbner basis for I. Then G is used as the private key for the system.

The public key consists of a set $Q = \{q_j\}_{j=1}^{s}$ of polynomials in the ideal I, which are chosen so that the computation of a Gröbner basis for $\langle Q \rangle$ is infeasible, and the message space M consists of polynomials, whose terms are not contained in $Lt(I)$, the leading term ideal of I, i.e. the message space M consists of polynomials that are reduced with respect to I.

Encryption is achieved by randomly choosing polynomials $h_1, h_2, \ldots, h_s \in K[X]$, setting $p = \sum_{j=1}^{s} h_j q_j$, and letting $c = p + m$ (where m is the message). Thus, the ciphertext is the sum of $p \in \langle Q \rangle \subset I$ and $m \notin I$, where m is reduced with respect to G. Since G is a Gröbner basis for I reducing c modulo G yields the unique remainder $N_G(c) = m$. Thus, the ciphertext, is decrypted by applying the multivariable division algorithm to $c = p + m$. On the other hand division by a set that is not a Gröbner basis does not yield a unique remainder. Thus, attempts at decryption by the public key, B will not (in theory) yield the correct plaintext message m. We note that the encryption here is probabilistic rather than deterministic.

To summarize, we have the following:

Private Key: A Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ for an ideal I of a polynomial ring $K[X]$ over a finite field K.

Public Key: A set $Q = \left\{ q_j : q_j = \sum_{i=1}^{s_j} h_{ij} g_i \right\}_{j=1}^{s} \subset I$ such that determining a Gröbner basis for $\langle Q \rangle$ is computationally infeasible.

Message Space: The set of all polynomials M that do not reduce to 0 modulo G.

Encryption: $c = p + m$, where $p = \sum_{j=1}^{m} h_j q_j$ is a polynomial in $J = \langle Q \rangle$ and $m \in M$ is a message.

Decryption: Reduction of c modulo G yields the message, m.

2.1 Noncommutative Gröbner bases

In this section, we present some background on the theory of noncommutative Gröbner bases, on which noncommutative Polly Cracker-type cryptosystems are based. Most of the theory is analogous to commutative Gröbner basis theory. However one significant difference is that unlike the commutative case, most ideals of noncommutative algebras do not have finite Gröbner bases. We refer the reader to [11] for details.

Let K be a finite field, and let $R = K\langle x_1, x_2, \ldots, x_n\rangle$ be the free associative algebra in n non-commuting variables. By a *monomial*, we mean a (finite) noncommutative word in the alphabet $\{x_1, x_2, \ldots, x_n\}$. We use the letter B to denote the set of monomials, and note that if $f \in R$, then f can be represented as $f = \sum_i \alpha_i b_i$, where $\alpha_i \in K$ with only finitely many $\alpha_i \neq 0$, and $b_i \in B$. If the coefficient of b_i in $f = \sum \gamma_j b_j$ is not zero, then b_i is said to *occur* in f. The set of all monomials that occur in f, is called the *support* of f, and is denoted $supp\,(f)$.

Next, we define multiplication in B by concatenation, and note that B is a multiplicative K-basis of R, i.e. B is a K-basis of R and $b, b' \in B$ implies that $b \cdot b' \in B$.

If $Y \subset R$, we use the symbol $\langle Y\rangle$ to denote the ideal generated by Y. We say that an ideal I in R is a *monomial ideal*, if it can be generated by elements of B.

A well-order $>$ on B is said to be *admissible* if it satisfies the following conditions for all $p, q, r, s \in B$:

1. if $p < q$ then $pr < qr$
2. if $p < q$ then $sp < sq$ and
3. if $p = qr$ then $p \geq q$ and $p \geq r$.

If $>$ is an admissible order on the monomials and $f \in R$, we say that b_i is the *tip* of f, denoted $\mathrm{tip}(f)$, if b_i occurs in f and $b_i \geq b_j$ for all b_j occurring in f. We denote the coefficient of $\mathrm{tip}(f)$ by $\mathrm{Ctip}(f)$. Furthermore, if $X \subseteq R$, then we write $\mathrm{Tip(X)} = \{b \in B : b = \mathrm{tip}(f)$ for some nonzero $f \in X\}$ and $\mathrm{NonTip}(X) = B \setminus \mathrm{Tip}(X)$.

Definition 2.1 If $>$ is an admissible order on $K\langle x_1, x_2, \ldots, x_n\rangle$, and I is a two-sided ideal of R, we say that $G \subset I$ is a *Gröbner basis* for I with respect to $>$ if $\langle \mathrm{Tip}(G)\rangle = \langle \mathrm{Tip}(I)\rangle$. Equivalently, $G \subset I$ is a Gröbner basis of I if for every $b \in \mathrm{Tip}(I)$, there is some $g \in G$ such that $\mathrm{tip}(g)$ divides b, i.e. for every $f \in I$ there exists $g \in G$, and $p, q \in B$ such that $p \cdot \mathrm{tip}(g) \cdot q = \mathrm{tip}(f)$.

We note that if I is an ideal of R, then $R = I \oplus \mathrm{Span}(\mathrm{NonTip}(I))$, as vector spaces over K. In particular, every nonzero $r \in R$ can be written uniquely as $r = i_r + N_I(r)$, where $i_r \in I$ and $N_I(r) \in \mathrm{Span}(\mathrm{NonTip}(I))$. $N_I(r)$ is called the *normal form* of r with respect to I.

Next, we define the concept of reduced (noncommutative) Gröbner bases. In order to do this, we note that if I is a monomial ideal of R, then I has a minimal monomial generating set. That is, there is a unique set of generators of I, none of which can be omitted and still generate I. We note, however, that this minimal monomial generating set need not be finite. This differs from the commutative case, in which Dickson's lemma [6] states that every monomial ideal of a commutative ring can be generated by a finite number of monomials. We are now ready to give the following:

Definition 2.2 Let I be an ideal in R, let I_{MON} be the ideal generated by $\mathrm{Tip}(I)$, and let T be the unique minimal monomial generating set of I_{MON}. Then the *reduced Gröbner basis* for I, is $G = \{t - N(t) : t \in T\}$.

The following properties of a reduced Gröbner basis are easy to see:

1. G is a Gröbner basis for I.
2. If $g \in G$ then the coefficient of $\mathrm{tip}(g)$ is 1.
3. If $g_i, g_j \in G$ with $g_i \neq g_j$, and b_i is any monomial that occurs in g_i, then $\mathrm{tip}\,(g_j)$ does not divide b_i.
4. If $g \in G$ then $g - \mathrm{tip}(g) \in \mathrm{Span}(\mathrm{NonTip}(I))$.
5. $\mathrm{Tip}(G)$ is the minimal monomial generating set for I_{MON}.

We also emphasize that in this setting, the reduced Gröbner basis of an ideal may be infinite. In fact, even finding partial Gröbner bases for many ideals seems intractable. These facts are used in the construction of noncommutative Polly Cracker-type cryptosystems.

Before presenting the system, we need the notion of reduction (division) of a polynomial g by a set of polynomials, which may be defined as follows:

Given an ordered subset, $F = \{f_1, f_2, \ldots, f_k\}$ of R, and $g \in R$, reducing (dividing) g by F means finding non-negative integers $t_1, t_2, \ldots, t_k$ and elements $u_{ij}, v_{ij}, r \in R$, for $1 \leq i \leq k$ and $1 \leq j \leq t_i$ such that:

1. $g = \sum_{i=1}^{k} \sum_{j=1}^{t_i} u_{ij} f_i v_{ij} + r$.
2. $\text{tip}(g) \geq \text{tip}(u_{ij} f_i v_{ij})$ for all i and j.
3. $\text{tip}(f_i)$ does not divide any monomial that occurs in r, for $1 \leq i \leq k$.

If $r \neq 0$, then $\text{tip}(r) \leq \text{tip}(g)$, and r is the remainder of the division.

As in the commutative case, the order on the set $F = \{f_1, f_2, \ldots, f_k\}$ affects the outcome of the division algorithm. However, if G is a Gröbner basis, then the remainder r of the division of f by G, is independent of the order of $g_1, g_2, \ldots, g_k$ in G.

2.2 Noncommutative Polly Cracker-type cryptosystems

[21] presents a class of cryptosystems whose security is based on the intractability of the ideal membership problem for a noncommutative free algebra over a finite field. In this section, we summarize the generic version of these cryptosystems, which form a noncommutative analogue of the Polly Cracker cryptosystem. We also summarize some of the techniques for determining private keys, which were originally presented in [21].

Let K be a finite field, and $R = K\langle x_1, x_2, ..., x_n\rangle$ be the noncommutative free algebra in n variables over K. Let I be a two-sided ideal of R, and suppose $G = \{g_1, g_2, \ldots, g_t\}$ is a finite Gröbner basis for I. Then G is used as the private key.

The public key, $Q = \{q_1, q_2, \ldots, q_s\}$, is a finite set of polynomials in I, which are constructed as follows: Given $G = \{g_1, g_2, \ldots, g_t\}$, fix $r \in \{1, 2, \ldots, s\}$. For each i, $1 \leq i \leq t$, suppose $d_{ir} \in \mathbb{N}$. For each i, r, j, $1 \leq i \leq t$, $1 \leq j \leq d_{ir}$, choose f_{rij}, $h_{rij} \in R$, and set $q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij}$. In addition, Q is constructed so that $J = \langle Q\rangle$ does not have a finite Gröbner basis, and such that finding a partial Gröbner basis for J is intractable. In this context, we have the following cryptosystem:

Private Key: A Gröbner basis, $G = \{g_1, g_2, \ldots, g_t\}$ for a two-sided ideal, I, of a noncommutative algebra $K\langle x_1, x_2, ..., x_n\rangle$ over a finite field, K.

Public Key: A set, $Q = \left\{ q_r : q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij} \right\}_{r=1}^{s} \subset I$, chosen so that $\langle Q \rangle$ does not have a finite Gröbner basis, and such that finding a partial Gröbner basis for J is intractable.
Message Space: The message space consists of polynomials that do not reduce to zero modulo I. i.e. $M \subseteq \{m \in R : supp\,(m) \in \mathrm{NonTip}(I)\}$, where $supp\,(f)$ is the support of f.
Encryption: $c = p+m$, where $m \in M$ is a message and $p = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij}$ is a polynomial in $J = \langle Q \rangle \subset I$. Here the F_{rij} and the H_{rij} are randomly chosen.
Decryption: Reduction of c modulo G yields the message, m.

Some simple examples of cryptosystems of this type that are presented in [21] include:

Example 2.3 Let K be a finite field, $K\langle x_1, x_2, \ldots, x_6 \rangle$ be the free algebra over K in six non-commuting variables. Let $Z = \prod_{i=1}^{6} x_i$ and $c_0, c_1, \ldots, c_6 \in K \setminus \{0\}$ be arbitrary constants. Set $g = Z + \sum_{i=1}^{6} c_i x_i + c_0 \in K\langle x_1, x_2, \ldots, x_6 \rangle$ as the private key. The public key $B = \{q_1, q_2\}$ consists of the polynomials $q_1 = fgh + hg$, $q_2 = hgf + gh$, where $f = X + \sum_{i=1}^{6} a_i x_i + a_0$, $h = Y + \sum_{i=1}^{6} b_i x_i + b_0 \in K\langle x_1, x_2, \ldots, x_6 \rangle$, $X = x_1 \cdot \prod_{i=2}^{5} \rho(x_i) \cdot x_6$, $Y = x_1 \cdot \prod_{i=2}^{5} \sigma(x_i) \cdot x_6$, where ρ, σ are distinct, nontrivial permutations of $\{x_2, x_3, x_4, x_5\}$, and $a_0, a_1, \ldots, a_6, b_0, b_1, \ldots, b_6 \in K$ are nonzero constants. In this setting, the message space $M \subseteq \mathrm{span}\,(\mathrm{NonTip}(\langle g \rangle))$ could consist of linear polynomials in $K\langle x_1, x_2, \ldots, x_6 \rangle$. Alternatively, fix $D \in \mathbb{N}$, then M could consist of univariate polynomials of degree $\leq D$ in one of the variables.

Example 2.4 Let K be a finite field, $K\langle x, y \rangle$ the noncommutative free algebra in two variables (over K). Let $\alpha, \beta, \gamma, \delta \in K$, and set $g = \alpha xy + \beta x + \gamma y + \delta$ as the private key. Since the public key has no direct effect on the attacks that we consider in this article, we omit its description here, and refer the reader to [21] for the same. As in the previous example, the message space, $M \subseteq \mathrm{span}\,(\mathrm{NonTip}(\langle g \rangle))$ could consist of linear polynomials. Alternatively, fix $D \in \mathbb{N}$. Then M could consist of univariate polynomials of degree $\leq D$ in one of the variables.

3 The Attack

Several issues related to the security of the commutative version of the Polly Cracker cryptosystem have been raised by [2], [8], [10], [12], and [22]. In the noncommutative case, some of these issues (e.g. linear algebra attacks) and possible countermeasures against them are discussed by [21]. The linear algebra attacks are ciphertext-only attacks, i.e. an attacker only has one ciphertext and tries to decipher it without determining or using the secret key. Even if such attacks are successful, they do not result in a total compromise of the system, since the attacker is only able to decrypt the ciphertext to which he/she has access - and that too, after a substantial amount of computation. In this section we what to address so-called chosen-ciphertext attacks. In these attacks, the attacker has access to the decryption device as a black box, i.e. he/she has the ability to decrypt a finite number of ciphertext messages, without actually knowing the details of the decryption algorithm. In this case, the attacker can encrypt carefully chosen messages using the public key, and then decrypt the corresponding ciphertest using his/her temporary access to the decryption black box. By using publicly known information to construct "chosen" ciphertext, which reveals parts of the private key, when decrypted, he/she is able to reconstruct a version of the private key in a finite number of steps. In the adaptive chosen-ciphertext attacks (discussed in section 6) the choice of ciphertext to generate depends on some previous information obtained by the attacker. We now describe a basic chosen-ciphertext attack against the cryptosystems presented in examples 2.3 and 2.4, which reveals the private key, thus completely compromising the security of these systems. We need the following

Definition 3.1 Let $f \in K\langle x_1, x_2, \ldots, x_n\rangle$. We define the *tail* of f by $\text{tail}(f) = f - \text{Ctip(f)} \cdot \text{tip(f)}$.

We begin by summarizing a simplified version of the attack, which is used to cryptanalyze the cryptosystems described in Examples 2.3 and 2.4:

Attack 3.2
Assumptions:

1. Alice's private key consists of a single polynomial, g, and $\text{tip}(g)$ is publicly known or can be easily determined from her public key.

2. The cryptanalyst, Catherine, has temporary access to Alice's decryption black box, i.e. Catherine is able to decrypt at least one

   ciphertext message that she sends, without actually knowing Alice's private key.

Method:

Catherine creates a fake ciphertext message, by encrypting tip(g). i.e. she constructs a ciphertext polynomial, $C = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + \text{tip(g)}$, where $Q = \{q_1, q_2, \ldots q_s\}$ is Alice's public key, and F_{rij}, H_{rij} are arbitrary polynomials. She then uses her temporary access to Alice's decryption black box to "decrypt" this pseudo-ciphertext. Since $\sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle g \rangle$, it vanishes, when reduced modulo g, and the output of the decryption algorithm (reduction of C modulo g) yields $f = \text{tip}(g) - [\text{Ctip}(g)]^{-1} \cdot g = -[\text{Ctip}(g)]^{-1} \cdot \text{tail}(g)$. Next, Catherine constructs $g' = \text{tip}(g) + [\text{Ctip}(g)]^{-1} \cdot \text{tail}(g)$. Since $\text{Ctip}(g) \cdot g' = \text{Ctip}(g) \cdot \text{tip}(g) + \text{tail}(g) = g$, it follows that $\langle g \rangle = \langle g' \rangle$, and that g' is a Gröbner basis for $\langle g \rangle$. Hence, Catherine can decrypt all of Alice's messages by using g', i.e. knowing g' has the same effect as knowing Alice's private key.

We next show that this attack works against any Polly Cracker-type cryptosystem (commutative or noncommutative), in which the private key is a reduced Gröbner basis, consisting of more than one polynomial. We now describe how such an attack might work:

Attack 3.3

Assumptions:

1. Alice's private key consists of a finite reduced Gröbner basis $G = \{g_1, g_2, \ldots g_m\}$.

2. tip(g_α) is publicly known for all $\alpha = 1, 2, \ldots m$, or can be easily determined from Alice's public key.

3. The cryptanalyst, Catherine, has temporary access to Alice's decryption black box, i.e. Catherine is able to decrypt a limited number of ciphertext messages that she sends, without actually knowing Alice's private key.

Method:

As in Attack 3.2, Catherine begins by constructing a "ciphertext" polynomial $C_1 = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + \mathrm{tip}(g_1)$, which encrypts the fake plaintext, $\mathrm{tip}\,(g_1)$. She then uses her temporary access to Alice's decryption black box to "decrypt" this pseudo-ciphertext. Once again, the enciphering polynomial, $\sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle G \rangle$ vanishes, when reduced modulo G. Moreover, since G is a reduced Gröbner basis, $\mathrm{tip}\,(g_\alpha)$ does not divide any monomial that occurs in $\mathrm{tail}\,(g_1)$ for any $g_\alpha = 2, 3, \ldots m$. So the output of the decryption algorithm (reduction of C_1 modulo G) yields $f_1 = \mathrm{tip}(g_1) - [\mathrm{Ctip}(g_1)]^{-1} \cdot g_1 = -[\mathrm{Ctip}(g_1)]^{-1} \cdot \mathrm{tail}(g_1)$. Next, Catherine constructs $g_1' = \mathrm{tip}(g_1) + [\mathrm{Ctip}(g_1)]^{-1} \cdot \mathrm{tail}(g_1)$. She repeats this process for each $\alpha = 1, 2, \ldots m$, and obtains a set, $G' = \{g_1', g_2', \ldots g_m'\}$, where $g_\alpha' = \mathrm{tip}(g_\alpha) + [\mathrm{Ctip}(g_\alpha)]^{-1} \cdot \mathrm{tail}(g_\alpha)\ \forall \alpha = 1, 2, \ldots m$. Since $\mathrm{Ctip}(g_\alpha) \cdot g_\alpha' = \mathrm{Ctip}(g_\alpha) \cdot \mathrm{tip}(g_\alpha) + \mathrm{tail}(g_\alpha) = g_\alpha\ \forall \alpha = 1, 2, \ldots m$, it follows that $\langle G \rangle = \langle G' \rangle$, and that G' is a Gröbner basis for $\langle G \rangle$. Hence, Catherine can decrypt all of Alice's messages by using G'. In fact, G' is an alternative version of Alice's private key.

We note that in most implementations of chosen-ciphertext attacks, it is a convention to disguise the fake message which is used. This is done to obscure the fact that the ciphertext contains some aspect of the private key hidden within it. One technique that can be used to do this in the case of the attacks that we have presented above, could be as follows:

Given $\mathrm{tip}(g_\alpha) \in \mathrm{Tip}(G)$, Catherine chooses polynomials t_α and s_α, such that $\mathrm{tip}\,(g_\beta)$ does not divide any monomial that occurs in $t_\alpha \cdot \mathrm{tip}\,(g_\alpha) \cdot s_\alpha$, for any $g_\beta \in G \setminus \{g_\alpha\}$. She then creates the pseudo-ciphertext, $C_\alpha = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + t_\alpha \cdot \mathrm{tip}\,(g_\alpha) \cdot s_\alpha$. Proceeding, as above, she uses her temporary access to Alice's decryption black box to "decrypt" the fake ciphertext, and obtains the plaintext $f = -[\mathrm{Ctip}(g_\alpha)]^{-1} t_\alpha \cdot \mathrm{tail}\,(g_\alpha) \cdot s_\alpha$. She then uses linear algebra, and her knowledge of t_α and s_α to deduce $-[\mathrm{Ctip}(g_\alpha)]^{-1} \cdot \mathrm{tail}\,(g_\alpha)$ from f_α, and constructs the polynomial, $g_\alpha' = \mathrm{tip}(g_\alpha) + [\mathrm{Ctip}(g_\alpha)]^{-1} \cdot \mathrm{tail}(g_\alpha)$. She proceeds with the rest of the attack, as above.

We note that the conditions on t_α and s_α are necessary to ensure that the fake ciphertext, C_α, decrypts to $-[\mathrm{Ctip}(g_\alpha)]^{-1} t_\alpha \cdot \mathrm{tail}\,(g_\alpha) \cdot s_\alpha$, and that none of its terms vanish during the decryption process. We note also that polynomials which satisfy this condition could exist in theory. This is due to the fact that G is a reduced Gröbner basis. So $\mathrm{tip}\,(g_\beta)$ does not divide $\mathrm{tip}\,(g_\alpha)$, for any $g_\beta \in G \setminus \{g_\alpha\}$. Furthermore, since $\mathrm{Tip}(G)$, does not contain

any monomials that are in the message space M the polynomials, t_α and s_α could be made up of monomials in M. This does not guarantee that the polynomials will satisfy the required condition, since it does not preclude the possibility that there exists some $\beta \neq \alpha$ such that $\mathrm{tip}\,(g_\beta)$ divides $t_\alpha \cdot \mathrm{tip}\,(g_\alpha)$ or $\mathrm{tip}\,(g_\alpha) \cdot s_\alpha$. However, in the absence of concrete examples, this is a good starting point if Catherine wishes to disguise the fake ciphertext. On the other hand an element of $\mathrm{Tip}(G)$ could always occur in a legitimate ciphertext polynomial, and any technique used to disguise the fact that $\mathrm{tip}\,(g_\alpha)$ is part of the message may be redundant.

4 Generalizing the attack

In view of the attacks presented in the previous section, one might be tempted to achieve security against chosen-ciphertext attacks, by designing a Polly Cracker-type cryptosystem, whose private key is a Gröbner basis which contains more than one polynomial, and which is not reduced. However, in this section, we show how the attack presented in section 3 can be used against a Polly Cracker-type cryptosystem, even if the private key is not a reduced Gröbner basis. First, we do this under the assumption that the tip set of the private key is publicly known or that it can be easily determined from publicly known information. In a second version of this attack, we also show how it can be used without knowledge of the tip set of the private key, if the admissible order used in the decryption algorithm is known.

Theorem 4.1

Any Polly Cracker-type cryptosystem is vulnerable to chosen-ciphertext attacks if the following conditions are satisfied:

1. *The private key consists of a finite Gröbner basis* $G = \{g_1, g_2, \ldots g_m\}$.
2. *tip*(g_α) *is publicly known or can be easily determined from publicly-known information for all* $g_\alpha \in G$, *where* $G = \{g_1, g_2, \ldots g_m\}$.
3. *The cryptanalyst has temporary access to the decryption black box.*

Proof.

Let $G = \{g_1, g_2, \ldots g_m\}$ be the private key. Then the public key is of the form $Q = \left\{q_r : q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij}\right\}_{r=1}^{s} \subset \langle G \rangle$. We show that

it is possible to construct an alternative version of the private key, if the conditions described in the theorem are met.

First, we encrypt the fake plaintext $\mathrm{tip}\,(g_1)$ by constructing a pseudo-ciphertext polynomial $C_1 = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + \mathrm{tip}(\mathrm{g}_1)$. We then use our temporary access to the decryption black box to "decrypt" this pseudo ciphertext. Since $Q \subset \langle G \rangle$, the enciphering polynomial $\sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle G \rangle$. Therefore, it vanishes, when reduced modulo G. Similarly, $\mathrm{tip}\,(g_1)$ vanishes, when reduced modulo G. In fact, the first step in the reduction of C_1 modulo G, yields $\mathrm{tip}(g_1) - [\mathrm{Ctip}(g_1)]^{-1} \cdot g_1 = -[\mathrm{Ctip}(g_1)]^{-1} \cdot \mathrm{tail}(g_1)$. Subsequent steps of the decryption algorithm then yield the same output as the reduction of g_1 modulo G. In other words, the output of the decryption algorithm yields $N_G(\mathrm{tip}\,(g_1))$. Next, we construct $g_1' = \mathrm{tip}(g_1) - N_G(\mathrm{tip}\,(g_1))$. As noted in the remarks preceding Definition 2.2, if I is an ideal and $r \neq 0$, then $i_r = r - N_I(r) \in I$. In particular, for $r = \mathrm{tip}(g_1)$ and $I = \langle G \rangle$, we have $g_1' = \mathrm{tip}(g_1) - N_G(\mathrm{tip}\,(g_1)) \in \langle G \rangle$.

Next, by repeating this process for each $\alpha = 1, 2, \ldots m$, we obtain a set $G' = \{g_1', g_2', \ldots g_m'\}$, where $g_\alpha' = \mathrm{tip}(g_\alpha) - N_G(\mathrm{tip}\,(g_\alpha))\ \forall \alpha = 1, 2, \ldots m$. By using the same argument as in the case of g_1', we see that $g_\alpha' \in \langle G \rangle\ \forall \alpha = 1, 2, \ldots m$, i.e. $\langle G' \rangle \subset \langle G \rangle$. Furthermore, $\mathrm{Tip}\,(G') = \mathrm{Tip}\,(G)$. It follows that $\langle G \rangle = \langle G' \rangle$, and that G' is a Gröbner basis for $\langle G \rangle$. In other words, G' is an alternative version of the private key, and we can decrypt all messages by using G'. $\diamond$

It is not completely clear *a priori* that it is easy for the attacker to obtain $\mathrm{Tip}(G)$. It is, however, possible to obtain it for the few examples of the noncommutative Polly Cracker that have been studied, and in the absence of concrete instances of the noncommutative Polly Cracker, in which $\mathrm{Tip}(G)$ is completely hidden, it seems reasonable to assume that attacker can actually obtain it. In any case the cryptosystem needs to be prepared for such kind of attacks.

In the next theorem however, we show that it is not necessary to know $\mathrm{Tip}(G)$, if the admissible order (see paragraph before Definition 2.1) used in the decryption algorithm is known. This version of the attack varies from the previous ones in that it uses ciphertexts created from the largest tip T of the polynomials in the public key, and monomials that are smaller than T under the admissible order used in the decryption algorithm. In fact, it requires no knowledge of the structure of the private key, and as such, is a significantly greater threat than the attacks described above.

Theorem 4.2

Any Polly Cracker-type cryptosystem is vulnerable to chosen-ciphertext attacks if the following conditions are satisfied:

1. *The private key consists of a finite Gröbner basis* $G = \{g_1, g_2, \ldots g_m\}$.
2. *The admissible order used in the decryption algorithm is publicly known.*
3. *The cryptanalyst has temporary access to the decryption black box.*

Proof.

Let $G = \{g_1, g_2, \ldots g_m\}$ be the private key. Then, the public key is of the form, $Q = \left\{q_r : q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij}\right\}_{r=1}^{s} \subset \langle G \rangle$. We show that it is possible to construct an alternative version of the private key, if the conditions described in the theorem are met.

First, since we know the admissible order used in the decryption algorithm, we can determine the largest tip T that occurs in public key Q. Next, since $Q \subset \langle G \rangle$, we know that $T \in \langle \mathrm{Tip}\,(G)\,\rangle$. Considering the structure of the polynomials in Q we also have that if $t \in \mathrm{Tip}(G)$, then $t \leq T$ (in practice, $t < T$). We begin by constructing a pseudo-ciphertext polynomial $C_T = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + T$, which encrypts the fake plaintext T. We then use our temporary access to the decryption black box to "decrypt" this pseudo-ciphertext. Once again, the enciphering polynomial $\sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle G \rangle$ vanishes, when reduced modulo G, and so does T. In fact, the output of the decryption algorithm is the same as the reduction of T modulo G. In other words, the output of the decryption algorithm yields $N_G\,(T)$. Next, we construct $g'_T = T - N_G\,(T)$. As noted in the remarks preceding Definition 2.2, if I is an ideal and $r \neq 0$, then $i_r = r - N_I(r) \in I$. In particular, for $r = T$ and $I = \langle G \rangle$, we have $g'_T = T - N_G\,(T) \in \langle G \rangle$.

We repeat this process for each $b \in B_T$, where B_T is the set of monomials which are $\leq T$, i.e. for each $b \in B_T$ we construct a pseudo-ciphertext polynomial, $C_b = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + b$, and use our temporary access to the decryption black box to "decrypt" the resulting pseudo-ciphertext. Now, for each $b \in B_T$, there are two possible results of the decryption process: if $b \in \langle \mathrm{Tip}\,(G)\,\rangle$, then the decryption process yields $N_G\,(b) \neq b$, and if $b \notin \langle \mathrm{Tip}\,(G)\,\rangle$, then the decryption process returns $N_G\,(b) = b$. If $b \in \langle \mathrm{Tip}\,(G)\,\rangle$, and the decryption process yields $N_G\,(b) \neq b$, we construct $g'_b = b - N_G\,(b)$, and if $b \notin \langle \mathrm{Tip}\,(G)\,\rangle$, we discard b. Since there are only a finite

number of monomials in B_T, this process ends in a finite number of steps, and we obtain the set $G' = \{g'_b = b - N_G(b) : b \in B_T \cap \langle \mathrm{Tip}(G) \rangle\}$. By using the same argument as in the case of g'_T, we see that $g'_b \in \langle G \rangle \; \forall b \in B_T \cap \langle \mathrm{Tip}(G) \rangle$. i.e. $\langle G' \rangle \subset \langle G \rangle$. Furthermore, $\mathrm{Tip}(G) \subset \mathrm{Tip}(G')$. It follows that $\langle G \rangle = \langle G' \rangle$, and that G' is a Gröbner basis for $\langle G \rangle$. Hence, G' is an alternative version of the private key, and we can decrypt all messages by using G'. $\diamond$

We note that although Theorems 4.1 and 4.2 are presented here in the notation and terminology of noncommutative Gröbner bases, they are equally valid against the generic commutative Polly Cracker cryptosystem.

Another point to note here is what we mean by vulnerability. In fact the Theorem above does not give us an efficient attack in the sense that it is not polynomial-time. What we do have, though, is the realistic attack scenario controlled by the parameter $|B_T|$, where $|B_T|$ is the cardinality of B_T. Thus in order to prevent such an attack one should take care that this parameter is high enough, so that searching through B_T is not feasible.

5 Countering the attack

As seen in the previous section, chosen-ciphertext attacks pose a serious threat to the Polly Cracker-type cryptosystems. However, in this section, we present a very simple technique to counter these attacks, by programming the decryption algorithm to recognize illegitimate ciphertexts, such as those required to execute these attacks. We then show how a similar technique can be used to counter an adaptive chosen- ciphertext attack that is described by [13].

We begin by presenting the following countermeasure, which can be used to secure noncommutative Polly Cracker-type cryptosystems from the chosen-ciphertext attacks presented above.

Countermeasure 5.1

1. *Restrict the message space, M, so that* $\mathrm{NonTip}(G) \setminus M \neq \emptyset$.
2. *Ensure that at least one monomial b_i occurs in each $g_i \in G$ such that $b_i \in \mathrm{NonTip}(G) \setminus M$ and $u \cdot b_i \cdot v \notin M$ for all $u, v \in B$.*
3. *Program the decryption algorithm to check whether any elements of* $\mathrm{NonTip}(G) \setminus M$ *occur in the normal form of a ciphertext polynomial after it has been reduced modulo the private key.*

4. *If the decryption algorithm encounters an element of* $\mathrm{NonTip}(G) \setminus M$ *in the normal form of a ciphertext polynomial, program it to return an error message (or the original ciphertext polynomial without reduction).*

For example, if $g = \alpha xy + \beta x + \gamma y + \delta$, as in Example 2.4, the message space could be restricted to linear polynomials in y. The decryption algorithm could be programmed to recognize the fact that any ciphertext which reduces to a polynomial containing x is not a legitimate ciphertext.

Similarly, if $g = x_1x_2x_3x_4x_5x_6 + \sum_{i=1}^{6} c_ix_i + c_0 \in K\langle x_1, x_2, \ldots, x_6\rangle$, as in Example 2.3 the message space could be restricted to linear polynomials in only some of the variables. For example, it could be restricted to linear polynomials in x_1, x_2, x_3, x_4, x_5 and exclude any polynomials that contain x_6. In this case, the decryption algorithm could be programmed to recognize the fact that any ciphertext which reduces to a polynomial that contains x_6 is not a legitimate ciphertext, and be programmed to return an error message, whenever it encounters such a ciphertext.

We note that in the versions of the cryptosystems presented in Examples 2.3 and 2.4, in which the message space M consists of univariate polynomials of degree $\leq D$ in one of the variables, where $D \in \mathbb{N}$ is fixed, Countermeasure 5.1 could be implemented without any modification of the message space.

Theorem 5.2 *Any Polly Cracker-type cryptosystem in which Countermeasure 5.1 is implemented, is secure against the chosen-ciphertext attacks which depend on the use of illegitimate ciphertexts to obtain the private key. In particular, it is secure against Attacks 3.2 and 3.3 and the attacks described in Theorems 4.1 and 4.2.*

Proof.

Suppose Countermeasure 5.1 is implemented in a Polly Cracker-type cryptosystem, and suppose an adversary has temporary black box access to the decryption black box. Suppose also, that this adversary uses the public key to encrypt a fake message m, which is not in the message space. Let C be the polynomial obtained by encrypting this illegitimate message m. Next, suppose that the adversary uses her temporary access to the decryption black box to decrypt C.

Let $G = \{g_1, g_2, \ldots g_t\}$ be the private key. We note that there exists some $g_i \in G$ and some monomial X which occurs in C, such that $\mathrm{tip}\,(g_i)$ divides X, i.e. $X = u_i \mathrm{tip}\,(g_i)\, v_i$ for some X which occurs in C, and some $g_i \in G$.

For, if no such X and g_i exist, then $C \in \mathrm{NonTip}(G)$ and dividing C by G has no effect on C. So running C through the decryption black box returns C if $C \in M$, or it returns an error message if $C \in \mathrm{NonTip}(G) \setminus M$.

Without loss of generality, we assume that $\mathrm{tip}\,(g_1)$ divides some monomial X_1 that occurs in C, and that X_1 is the largest such monomial that occurs in C. i.e. if Y is some other monomial that occurs in C with the property that $Y = u_i \mathrm{tip}\,(g_i)\, v_i$ for some $g_i \in G$, then $X_1 \geq Y$. Next, suppose $X_1 = u_1 \mathrm{tip}\,(g_1)\, v_1$. Then, in the first step of the division algorithm, C is reduced to $C_1 = C - Ctip\,(g_1)^{-1} \cdot a_1 \cdot u_1 \mathrm{tip}\,(g_1)\, v_1 \cdot g_1$, where $Ctip\,(g_1)$ is the coefficient of the $\mathrm{tip}\,(g_1)$, and a_1 is the coefficient of X_1 in C. Now, item 2 of Countermeasure 5.1 guarantees that a monomial, b_1 occurs in g_1 such that $b_1 \in \mathrm{NonTip}(G) - M$, and $u \cdot b_1 \cdot v \notin M$, for all $u, v \in B$. Therefore, the monomial $u_1 \cdot b_1 \cdot v_1$ occurs in C_1 and $u_1 \cdot b_1 \cdot v_1 \notin M$.

Next, if there is no $g_i \in G$ such that $\mathrm{tip}\,(g_i)$ divides some monomial X that occurs in C_1, then $u_1 \cdot b_1 \cdot v_1 \notin M$ occurs in $C_1 = N_G\,(C)$, and the decryption algorithm returns an error message as specified by items 3 and 4 of Countermeasure 5.1. If on the other hand, $\mathrm{tip}\,(g_i)$ divides some monomial X that occurs in C_1 for some $g_i \in G$, then the division algorithm proceeds as above, with a monomial of the form $u_\alpha \cdot b_\alpha \cdot v_\alpha$ being introduced into the polynomial C_α which is obtained as the reduced form of the ciphertext polynomial at the end of the α^{th} step of the algorithm. Since G is a finite Gröbner basis, the division algorithm ends in a finite number of steps, yielding $N_G\,(C)$. Now, if $g_\nu \in G$ is the polynomial used in the final step of the division C by G, then it is clear that $u_\nu b_\nu v_\nu$ occurs in $N_G\,(T)$ and $u_\nu b_\nu v_\nu \notin M$. So the decryption algorithm detects this monomial in $N_G\,(C)$, and returns an error message or the original polynomial, without reducing it.

Hence, any Polly Cracker-type cryptosystem, in which Countermeasure 5.1 is implemented is secure against chosen-ciphertext attacks which depend on the use of illegitimate ciphertexts to obtain the private key. In particular, it is secure against the chosen ciphertext attacks that are described in Attacks 3.2 and 3.3 and in Theorems 4.1 and 4.2. $\diamond$

Next, we consider an adaptive chosen-ciphertext attack, which uses legitimate ciphertext in its *modus operandi*. We begin by describing the attack, which appears in [13], chapter 5, section 3, exercise 11, page 110.

Attack 5.3 *([13])*

Suppose that two companies, Bob's company, and Catherine's company are communicating with Alice's company, using Alice's public key. On many

questions, Catherine is cooperating with Alice, but there is one extremely important customer who is taking competing bids from a group of companies led by Alice and Bob, and from a different consortium led by Catherine. Catherine knows that Bob has just sent Alice the encrypted amount of their bid, and she desperately wants to know what it is. Suppose that Bob's message m is sent as ciphertext c and that Catherine is able to see the ciphertext c. Catherine creates ciphertext $c' = p + c + m_0$, where $p = \sum_{i=1}^{s} F_i q_i$ is an encrypting polynomial and m_0 is an arbitrary element of the message space. She then sends c' to Alice, supposedly part of the message on an unrelated subject. She then informs Alice that she had a computer problem due to which she lost her plaintext, and she thinks that an incomplete message was encrypted for Alice. Could Alice please send her the decrypted message m' that she obtained from c', so that Catherine can reconstruct the correct message and re-encrypt it? Since p vanishes during the decryption process, and c decrypts to m it follows that c' decrypts to $m' = m + m_0$. So Catherine is able to use m' to find $m = m' - m_0$. Alice is willing to give Catherine m', because she is unable to see any connection between c' and c or between m' and m, and because Catherine's request seems reasonable when they are exchanging messages about a matter on which they are cooperating.

We note that the ciphertext c' sent by Catherine in Attack 5.3 is a legitimate ciphertext, thus making it difficult for Alice (or her decryption algorithm) to recognize it as a security threat. However, the richness of the message spaces of noncommutative Polly Cracker-type cryptosystems enables us to develop a technique that is similar to Countermeasure 5.1 to overcome this attack. We present this technique next.

Countermeasure 5.4

1. Alice chooses a private key G and develops a public key such that the message space M contains several polynomials, and can be partitioned into disjoint sets.

2. She picks $M_{Bob} \subset M$ and $M_{Catherine} \subset M$, such that $M_{Bob} \cap M_{Catherine} = \emptyset$.

3. She assigns M_{Bob} as Bob's message space and $M_{Catherine}$ as Catherine's message space.

For example, suppose Alice chooses a private key based on Example 2.3, i.e. suppose her private key consists of a single polynomial of the form $g = x_1x_2x_3x_4x_5x_6 + \sum_{i=1}^{6} c_ix_i + c_0 \in K\langle x_1, x_2, \ldots, x_6\rangle$. She then implements Countermeasure 5.1 by leaving all monomials that contain x_6 out of her message space, thus securing her private key from attacks that use illegitimate ciphertexts, such as the ones described in the previous sections. Next she assigns the variable x_1 to Bob and x_2 to Catherine, i.e. Bob's message space M_{Bob} consists of univariate polynomials in x_1 of degree d, where $0 < d \leq D$, and Catherine's message space $M_{Catherine}$ consists of univariate polynomials in x_2 of degree d, where $0 < d \leq D$, where $D \in \mathbb{N}$ is fixed. Note that in this scenario, constants in the field K, are not legitimate messages.

Now, if Catherine sends Alice a ciphertext c', which decrypts to $m' \in M_{Bob}$, it would immediately make Alice suspicious of Catherine's intentions. On the other hand, if Catherine sends Alice a ciphertext of the form $c' = p + c + m_0$, where c is a ciphertext used to encrypt a message $m \in M_{Bob}$ and $m_0 \in M_{Catherine}$, c' would reduce to an element of NonTip(G), which is neither in $M_{Catherine}$ nor in M_{Bob}, and would immediately draw Alice's attention to the suspicious nature of Catherine's ciphertext.

As was pointed out to us by the anonymous referee, Catherine can undertake the following attack. She can send a ciphertext $c' = b \cdot c$, where $b \in K$ is a constant. Then upon decryption she obtains $m' = b \cdot m$ and thus m itself. We note, however, that if Countermeasure 5.4 is implemented, we still have $m' = b \cdot m \in M_{Bob}$, which would make Alice suspicious of the message she received from Catherine.

Before ending this section, we note that Countermeasure 5.4 introduces an element of symmetric key encryption into the cryptosystem. However, it differs from traditional symmetric key schemes, in that there is no need for M_{Bob} or $M_{Catherine}$ to be kept secret. Thus the scheme remains, in essence, a public key cryptosystem.

6 Conclusion

In the present work we have shown how one can use the theory of noncommutative Gröbner bases to construct a public key cryptosystem. We have also presented some attacks that can be undertaken against such a system. The chosen ciphertext attacks described in this article are a serious concern and should be taken into consideration in the design of a noncommutative Polly

Cracker-type cryptosystems. However, they do not appear to be a major threat to the security of the system, since they can be easily countered by a minor modification to the decryption algorithm. In fact, even the simple examples that were presented in [21] can be made secure against chosen-ciphertext attacks by implementing the countermeasures proposed above. We believe that these attacks and the techniques to counter them, are small steps in an evolutionary process leading towards the development of a secure cryptosystem.

Acknowledgements

Both authors would like to acknowledge the support and inspiration provided by the Special Semester on Groebner Bases, February 1 - July 31, 2006, organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria.

The second author would also like to thank "Cluster of Excellence in Rhineland-Palatinate" for partially funding his research, and also personally his Ph.D. supervisor Prof.Dr. Gert-Martin Greuel and his second supervisor Prof.Dr. Gerhard Pfister for continuous support. He also would like to thank Viktor Levandovskyy and the anonymous referees for useful discussions and comments.

References

[1] P. Ackermann and M. Kreuzer. Gröbner basis cryptosystems. *AAECC*, 17(3–4):173–194, aug 2006.

[2] Boo Barkee, Deh Cac Can, Julia Ecks, Theo Moriarty, and R.F. Ree. Why you cannot even hope to use Gröbner bases in public key cryptology: An open letter to a scientist who failed and a challenge to those who have not yet failed. *Jour. Symb. Comput*, 18:497–501, 1994.

[3] M. Belllare and P. Rogaway. Optimal asymetric encryption - how to encrypt with RSA. In A.D.Santis, editor, *Advances in Cryptology - EUROCRYPT'96, Lecture Notes in Computer Science*, volume 950, pages 92–111. Springer Verlag, 1995.

[4] B. Buchberger. Gröbner bases: an algorithmic method in polynomial ideal theory. In N.K.Bose, editor, *Recent trends in multidimensional system theory*, pages 184–232. 1985.

[5] S. Bulygin. Chosen-ciphertext attack on noncommutative Polly Cracker. 2005.

[6] L. Dickson. Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *Amer. J. Math.*, (35):413–426, 1913.

[7] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. In *STOC*, 1991.

[8] R. Endsuleit, W. Geiselmann, and R. Steinwandt. Attacking a polynomial-based cryptosystem: Polly Cracker. *Int. Jour. Information Security*, (1):143–148, 2002.

[9] M. Fellows and N. Koblitz. Combinatorial cryptosystems galore! *Contemporary Math.*, (168):51–61, 1994.

[10] W. Geiselmann and R. Steinwandt. Cryptanalysis of Polly Cracker. *IEEE Trans. Information Theory*, (48):2990–2991, 2002.

[11] E. L. Green. Noncommutative Gröbner bases, and projective resolutions. In *Computational methods for representations of groups and algebras. Papers from the First Euroconference held at the University of Essen*, number 173, chapter 2, pages 29–60. Birkhäuser Verlag, 1999.

[12] D. Hofheinz and R. Steinwandt. A "Differential" Attack on Polly Cracker. In *IEEE Int. Symp. Information Theory*, page 211, 2002.

[13] N. Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computations in Math.* Springer, 1997.

[14] F. Levy-dit-Vehel and L. Perret. A Polly Cracker system based on satisfiability. In *Coding, Cryptography and Combinatorics, Progress in Computer Science and Applied Logic*, volume 23, pages 177–192. Birkhäuser Verlag, 2004.

[15] L. Ly. Polly two – a new algebraic polynomial-based public-key scheme. *AAECC*, 17(3–4), aug 2006.

[16] L. Van Ly. *Polly Two – A Public Key Cryptosystem based on Polly Cracker*. PhD thesis, Rhur Universität Bochum, Germany, 2002.

[17] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of applied cryptography*. CRC Press, 1997.

[18] T. Mora. Gröbner bases for noncommutative polynomial rings. In *Proc. AAECC, Lecture Notes in Computer Science*, volume 229, pages 353–362. 1986.

[19] T. Okamoto and D. Pointcheval. REACT: Rapid Enhanced-security Asymetric Encryption Transform. In D.Naccache, editor, *CT – RSA'2001, Lecture Notes in Computer Science*, volume 2020, pages 159–175. Springer Verlag, 2001.

[20] C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Crypto*, 1991.

[21] T. Rai. *Infinite Gröbner bases and noncommutative Polly Cracker cryptosystems*. PhD thesis, Virginia Tech, 2004.

[22] R. Steinwandt and M.I.G. Vasco. Chosen ciphertext attacks as common vulnerability of some group- and polynomial-based encryption schemes. In *WartaCrypt*, 2004.