COUNTERING CHOSEN-CIPHERTEXT ATTACKS AGAINST NONCOMMUTATIVE POLLY CRACKER-TYPE CRYPTOSYSTEMS.

TAPAN S. RAI

Abstract. In [2], Stanislav Bulygin presents a chosen-ciphertext attack against certain instances of noncommutative polly cracker-type cryptosystems which were proposed in [7] and [9]. In this article, we present generalized versions of this attack, which can be used against virtually all polly cracker-type cryptosystems. We then present a simple but effective techique to counter these attacks. We also present a technique to counter an adaptive chosen-ciphertext attack which was first described by Neil Koblitz in [8].

1. Preliminaries

1.1. **Noncommutative Gröbner bases.** We begin with some background on the theory of noncommutative Gröbner bases, on which noncommutative polly cracker-type cryptosystems are based. Most of the theory is analagous 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 [6] for details.

Let K be a finite field, and let $K\langle x_1, x_2, \ldots, x_n\rangle$ 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 $f \in K\langle x_1, x_2, \ldots, x_n\rangle$, 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.

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 $b \cdot b' \in B$. We say that an ideal I in $K\langle x_1, x_2, \ldots, x_n\rangle$ 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 $>$ be an admissible order on the monomials and $f \in K\langle x_1, x_2, \ldots, x_n\rangle$, 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 $X \subseteq K\langle x_1, x_2, \ldots, x_n\rangle$, then we write $\mathrm{Tip(X)} = \{b \in B : b = \mathrm{tip}(f)$ for some nonzero $f \in X\}$ and $\mathrm{NonTip}(X) = B - \mathrm{Tip}(X)$.

Date: September 24, 2005.

Definition 1.1. If $>$ be an admissible order on $K\langle x_1, x_2, \ldots, x_n\rangle$, and I is a two-sided ideal of $K\langle x_1, x_2, \ldots, x_n\rangle$. 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 for any ideal I, $K\langle x_1, x_2, \ldots, x_n\rangle = I \oplus \mathrm{Span}(\mathrm{NonTip}(I))$, as vector spaces. In particular, every nonzero $r \in K\langle x_1, x_2, \ldots, x_n\rangle$ 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 $K\langle x_1, x_2, \ldots, x_n\rangle$, 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 [5] proves 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 1.2. Let I be an ideal in $K\langle x_1, x_2, \ldots, x_n\rangle$, 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) $g \in G$ 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 not be finite – a fact that is 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 $K\langle x_1, x_2, \ldots, x_n\rangle$, and $g \in K\langle x_1, x_2, \ldots, x_n\rangle$, 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. $\mathrm{tip}(g) \geq \mathrm{tip}(u_{ij} f_i v_{ij})$ for all i and j.
3. $\mathrm{tip}(f_i)$ does not divide any monomial that occurs in r, for $1 \leq i \leq k$.

If $r \neq 0$, then $\mathrm{tip}(r) \leq \mathrm{tip}(g)$, 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.

1.2. **Noncommutative polly cracker-type cryptosystems.** In [7] and [9] we presented 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 M. Fellows' and N. Koblitz's polly cracker cryptosystem [4]. We also summarize some of the techniques for determining private keys, which were originally presented in [7] and [9].

Let K be a finite field, and $K\langle x_1, x_2, ..., x_n\rangle$ be the noncommutative free algebra in n variables over K. Let I be a two-sided ideal of $K\langle x_1, x_2, ..., x_n\rangle$, 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 $f_{rij},\ h_{rij} \in K\langle X\rangle$, 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. 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.

Message Space: $M = \mathrm{NonTip}(I)$ or a subset of $\mathrm{NonTip}(I)$.

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 we presented in [7] and [9] include:

Example 1.3. *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 $c_0, c_1, \ldots, c_6 \in K - \{0\}$ 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, $M \subseteq \mathrm{NonTip}(\langle g\rangle)$ 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 homogeneous polynomials of degree $\leq D$ in one of the variables.*

Example 1.4. *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 attack that we consider in this article, we omit its description here, and refer the reader to* [7] *or* [9] *for the same. As in the previous example, the message space, $M \subseteq \mathrm{NonTip}\left(\langle g\rangle\right)$ could consist of linear polynomials. Alternatively, fix $D \in \mathbb{N}$. Then M could consist of homogeneous polynomials of degree $\leq D$ in one of the variables.*

2. The Attack

In [2], Stanislav Bulygin describes a chosen ciphertext attack against polly cracker-type cryptosystems, which reveals the private key, thus completely compromising the security of the system. He goes on to assert that the attack could also be used against any polly cracker-type cryptosystem, in which the private key is a reduced Gröbner basis. In this section we summarize the attack given in [2] and present some of our comments on it. We need the following:

Definition 2.1. 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 1.3 and 1.4:

Attack 2.2.

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 $\text{tip}(g)$. i.e. she constructs a ciphertext polynomial, $C = \sum_{i=1}^{s}\sum_{j=1}^{k_{ir}} F_{rij}q_iH_{rij} + \text{tip(g)}$, 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 $\sum_{i=1}^{s}\sum_{j=1}^{k_{ir}} F_{rij}q_iH_{rij} \in \langle g\rangle$, 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.

Bulygin [2] describes a somewhat more complicated version of this attack, in which he suggests encrypting a disguised version of $\text{tip}(g)$, presumably to prevent the decryption algorithm from recognizing the fact that $\text{tip}(g)$ occurs in the ciphertext polynomial C. To do this he suggests finding polynomials, $t, s \in K\langle x_1, x_2, ..., x_n\rangle$ such that no monomial of $t \cdot \text{tip}(g) \cdot s$ is divisible by $\text{tip}(g)$. The ciphertext polynomial, C, is then constructed as $C = \sum_{j=1}^{k_{ir}} F_{rij}q_iH_{rij} + t \cdot \text{tip}(g) \cdot s$. Bulygin [2] asserts that finding polynomials s, t which satisfy the desired property is fairly easy. We note, however, that this is not the case, and in fact, that no such polynomials exist, since by its very construction, every monomial of $t \cdot \text{tip}(g) \cdot s$ is divisible by $\text{tip}(g)$. However, this appears to have no bearing on the attack, since the version described above appears to be legitimate in the sense that it would work under the very reasonable assumptions that are required to execute it.

Moreover, we believe that there is no real need to disguise the fact that $\text{tip}(g)$ occurs in the ciphertext polynomial C, since it could in fact occur even in a legitimate ciphertext polynomial. For example, if Alice's private key, g, is of the form

used in example 1.3, then $\text{tip}(g) = x_1x_2x_3x_4x_5x_6$, and all linear terms occur in the polynomials in the public key. So if the monomial $x_2x_3x_4x_5x_6$ occurs in any of the polynomials, H_{rij} used in encryption, $\text{tip}(g)$ would occur in the ciphertext polynomial, C. In fact, this is only one of many ways in which $\text{tip}(g)$ could occuur in a legitimate ciphertext polynomial. Similarly, if Alice's private key, g, is of the form $g = \alpha xy + \beta x + \gamma y + \delta$, as in example 1.4, then $\text{tip}(g) = xy$. Once again, all linear terms occur in the public key, and $\text{tip}(g)$ would occur in a legitimate ciphertext polynomial, if x occurred in one of the encrypting polynomials F_{rij}, or if y occurred in one of the encrypting polynomials, H_{rij}.

Bulygin [2] also asserts that this this attack could work 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 2.3.

Assumptions:

(1) Alice's private key consists of a reduced Gröbner basis, $G = \{g_1, g_2, \dots g_m\}$.
(2) $\text{tip}(g_\alpha)$ is publicly known for all $\alpha = 1, 2, \dots m$, 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 2.2, Catherine begins by constructing a "ciphertext" polynomial, $C_1 = \sum_{i=1}^{s}\sum_{j=1}^{k_{ir}} F_{rij}q_iH_{rij} + \text{tip}(\text{g}_1)$, which encrypts the fake plaintext, $\text{tip}\,(g_1)$. She then uses her temporary access to Alice's decryption black box to "decrypt" this pseudo ciphertext. Once again, the enciphering polynomial, $\sum_{i=1}^{s}\sum_{j=1}^{k_{ir}} F_{rij}q_iH_{rij} \in \langle G\rangle$ vanishes, when reduced modulo G. Morover, since G is a reduced Gröbner basis, $\text{tip}\,(g_\alpha)$ does not divide any monomial that occurs in $\text{tail}\,(g_1)$ for any $g_\alpha = 2, 3, \dots m$. So the output of the decryption algorithm (reduction of C modulo G) yields $f_1 = \text{tip}(g_1) - [\text{Ctip}(g_1)]^{-1} \cdot g_1 = -[\text{Ctip}(g_1)]^{-1} \cdot \text{tail}(g_1)$. Next, Catherine constructs $g_1' = \text{tip}(g_1) + [\text{Ctip}(g_1)]^{-1} \cdot \text{tail}(g_1)$. She repeats this process for each $\alpha = 1, 2, \dots m$, and obtains a set, $G' = \{g_1', g_2', \dots g_m'\}$, where $g_\alpha' = \text{tip}(g_\alpha) + [\text{Ctip}(g_\alpha)]^{-1} \cdot \text{tail}(g_\alpha)\ \forall\alpha = 1, 2, \dots m$. Since $\text{Ctip}(g_\alpha) \cdot g_\alpha' = \text{Ctip}(g_\alpha) \cdot \text{tip}(g_\alpha) + \text{tail}(g_\alpha) = g_\alpha\ \forall\alpha = 1, 2, \dots m$, 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'. i.e. knowing G' has the same effect as knowing Alice's private key.

We note that unlike the situation with attack 2.2, it might actually be possible to disguise the fake plaintext, $\text{tip}\,(g_\alpha)$, by using a modification of the technique that fails to do the same for attack 2.2. This could work as follows:

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

$g'_\alpha = \text{tip}(g_\alpha) + [\text{Ctip}(g_\alpha)]^{-1} \cdot \text{tail}(g_\alpha)$. 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 $-[\text{Ctip}(g_\alpha)]^{-1} t_\alpha \cdot \text{tail}(g_\alpha) \cdot s_\alpha$, and that none of its terms vanish during the decryption proocess. We note also that polynomials which satisy this condition could exist in theory. This is due to the fact that G is a reduced Gröbner basis. So $\text{tip}(g_\beta)$ does not divide $\text{tip}(g_\alpha)$, for any $g_\beta \in G - \{g_\alpha\}$. Furthermore, since $\text{Tip}(G)$, 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 $\text{tip}(g_\beta)$ divides $t_\alpha \cdot \text{tip}(g_\alpha)$ or $\text{tip}(g_\alpha) \cdot s_\alpha$. However, in the absence of concrete examples, this is a good starting point, if Catherine wishes to diguise the fake ciphertext. On the other hand, as we pointed out earlier, an element of $\text{Tip}(G)$ could always occur in a legitimate ciphertext polynomial, and any technique used to diguise the fact that $tip(g_\alpha)$ is part of the message may be redundant.

We also note that the *lunchtime attacks* of [3] are a version of attack 2.3, as applied to a private key consisting of linear polynomials.

3. 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 2 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 by Alice's decryption algorithm is known.

Attack 3.1.
Assumptions:

(1) Alice's private key consists of a finite Gröbner basis, $G = \{g_1, g_2, \ldots g_m\}$.
(2) $\text{tip}(g_\alpha)$ 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 the previous attacks 2.2 and 2.3, Catherine begins by constructing a "ciphertext" polynomial, $C_1 = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + \text{tip}(\text{g}_1)$, which encrypts the fake plaintext, $\text{tip}(g_1)$. 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, and so does $\text{tip}(g_1)$. In fact, the output of the decryption algorithm is the same as the reduction of g_1 modulo G. In other words, the output of the decryption algorithm yields $N_G(\text{tip}(g_1))$. Next, Catherine constructs $g'_1 = \text{tip}(g_1) - N_G(\text{tip}(g_1))$.

As noted in the remarks preceding definition 1.2, if I is an ideal and $r \neq 0$, then $i_r = r - N_I(r) \in I$. In particular, for $r = \text{tip}(g_1)$ and $I = \langle G \rangle$, we have $g'_1 = \text{tip}(g_1) - N_G(\text{tip}(g_1)) \in \langle G \rangle$.

She repeats this process for each $\alpha = 1, 2, \ldots m$, and obtains a set, $G' = \{g'_1, g'_2, \ldots g'_m\}$, where $g'_\alpha = \text{tip}(g_\alpha) - N_G(\text{tip}(g_\alpha)) \ \forall \alpha = 1, 2, \ldots m$. 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, $\text{Tip}(G') = \text{Tip}(G)$. 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.

Although this attack works under the assumptions required to execute it, we note that in the absence of concrete examples of noncommutative polly cracker-type cryptosystems, whose private keys consist of more than one polynomial, it is not clear whether the assumption that $\text{Tip}(G)$ can be easily determined from publicly known information is a reasonable one.

In the next version of this attack, however, we show that it is not necessary to know $\text{Tip}(G)$, if the monomial order used by Alice's decryption algorithm is known.

Attack 3.2.
Assumptions:

(1) Alice's private key consists of a finite Gröbner basis, $G = \{g_1, g_2, \ldots g_m\}$.
(2) The monomial order used in Alice's decryption algorithm is publicly known.
(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:

Since Catherine does not know the tips that occur in Alice's private key, she needs to use a different approach this time. She does, however, know Alice's monomial order, and uses it to determine the largest tip, T, that occurs in Alice's public key. Since Alice's public key, Q, is contained in the ideal, $I = \langle G \rangle$, generated by the private key, G, Catherine knows that $T \in \langle \text{Tip}(G) \rangle$, and that if $t \in \text{Tip}(G)$, then $t \leq T$ (in practice, $t < T$). Catherine begins by constructing a "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. 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, 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, Catherine constructs $g'_T = T - N_G(T)$. As noted earlier (in attack 3.1), we have $g'_T = T - N_G(T) \in \langle G \rangle$.

She repeats this process for each $b \in B_T$, where B_T is the set of monomials which are $\leq T$. i.e. for each, $b \in B_T$, she constructs a ciphertext polynomial, $C_b = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + b$, and uses her temporary access to Alice's 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 $b \in \langle \text{Tip}(G) \rangle$, then the decryption process yields $N_G(b) \neq b$, and if $b \notin \langle \text{Tip}(G) \rangle$, then the decryption process returns $N_G(b) = b$. If $b \in \langle \text{Tip}(G) \rangle$, and the decryption process yields $N_G(b)$, Catherine constructs $g'_b = b - N_G(b)$, and if $b \notin \langle \text{Tip}(G) \rangle$, she discards b. Since there are only

a finite number of monomials in B_T, this process ends in a finite number of steps, and she obtains 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, 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 note, that, although these attacks (3.1 and 3.2) are presented here in the notation and terminology of noncommutative Gröbner bases, they are equally valid against the generic commutative polly cracker cryptosystem.

4. Countering the attack

In view of the attacks described above, especially the versions in section 3, it would appear that the future of polly cracker-type cryptosystems is very bleak. 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 due to Koblitz [8].

Before doing this however, we note, once again, that in the absence of concrete examples, it is not clear whether the assumptions required to execute these attacks are reasonable. Specifically, in the case of attacks 2.3 and 3.1, it is not clear whether it is reasonable to assume that it would be possible to use publicly known information to easily determine $\mathrm{Tip}(G)$. Similarly, in the case of attack 3.2, it is not clear whether the assumption that the admissible order used in Alice's decryption algorithm is publicly known is a reasonable one. This is due to the fact that there are an uncountable number of admissible orders on any set of monomials. However, in practice, only a few orders are considered practical, since reduction (division) with respect to many block orders is very expensive.

Countermeasure 4.1.

(1) Restrict the message space, M, such that $\mathrm{NonTip}(G) - M \neq \emptyset$.
(2) Ensure that at least one monomial, b_i, occurs in each $g_i \in G$, such that $b_i \in \mathrm{NonTip}(G) - M$, 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 $\mathrm{NonTip}(G) - M$ occur in a 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 $\mathrm{NonTip}(G) - M$ 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 1.2, 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 $g = x_1x_2x_3x_4x_5x_6 + \sum_{i=1}^{6} c_i x_i + c_0 \in K\langle x_1, x_2, \ldots, x_6 \rangle$, as in example 1.1 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 ciphetext.

We note that in the versions of the cryptosystems presented in examples 1.1 and 1.2, in which the message space, M, consists of homogeneous polynomials of degree $\leq D$ in one of the variables, where $D \in \mathbb{N}$ is fixed, countermeasure 4.1 could be implemented without any modification of the message space.

It is clear that implementing countermeasure 4.1 in any polly cracker attack will defeat all of the attacks described in sections 2 and 3. For, if Catherine encrypts $\mathrm{tip}\,(g_1)$, as in attacks 2.2, 2.3 and 3.1, then the first step of the decryption process will yield $f_1 = \mathrm{tip}\,(g_1) - \mathrm{Ctip}\,(g_1)^{-1}\, g_1 = -\mathrm{Ctip}\,(g_1)^{-1}\,\mathrm{tail}\,(g_1)$. Now, since there is at least one monomial, $b_1 \in \mathrm{NonTip}(G) - M$, which occurs in g_1, this monomial also occurs in f_1. Furthermore, since $b_1 \in \mathrm{NonTip}(G)$, it is not affected by subsequent steps in the reduction, and hence, it occurs in the $N_G\,(\mathrm{tip}\,(g_1))$, which is the final form of the polynomial after the reduction process in the decryption algorithm. The decryption algorithm then detects b_1 occurring in the reduced polynomial and returns an error message or the original polynomial, without reducing it.

Similarly, if Catherine encrypts the tip, T, of a polynomial that occurs in Alice's public key, as in attack 3.2, then each step of the division algoritm introduces a monomial of the form $u_\alpha \cdot b_\alpha \cdot v_\alpha$ into the polynomial, f_α, which is obtained as the reduced form of the ciphertext polynomial at the end of the α^{th} step. Since G is a finite Gröbner basis, the division algorithm ends in a finite number of steps, yielding $N_G\,(T)$. Now, if $g_\nu \in G$ is the polynomial used in the final step of the division of Catherine's pseudo ciphertext polynomial 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 $N_G\,(T)$, and returns an error message or the original polynomial, without reducing it.

Hence, any polly cracker-type cryptosystem, in which countermeasure 4.1 is implemented is secure against the chosen-ciphertext attacks that are described in sections 2 and 3. Moreover, it seems reasonable to believe that their ability to recognize fake ciphertexts would make them secure against all chosen-ciphertext attacks that use pseudo-ciphertext.

In the rest of this secction, we consider an adaptive chosen-ciphertext attack, which uses legitimate ciphertext in its *modus operandi*. We begin by describing the attack, which first appeared in [8], chapter 5, section 3, exercise 11, page 110.

Attack 4.2. *(Koblitz* [8]*)*
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 desparately 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' 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,

lost her plaintext, ans thinks that an incomplete sequence of bits was encrypted for Alice. Could Alice please send her the decrypted bits 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 be Catherine in attack 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 the noncommutative polly-cracker-type cryptosystems enables us to develop a technique that is similar to countermeasure 4.1 to overcome this attack. We present this technique next.

Countermeasure 4.3.

(1) Alice chooses a private key, G, and develops a public key such that the message space, M, contains several monomials, 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 1.3. 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 4.1 by leaving all monomials that contain x_6 out of her message space, thus securing her private key from attacks of the type described in sections 3 and 4. Next she assigns the variable x_1 to Bob and x_2 to Catherine. i.e. Bob's message space, M_{Bob} consists of homogeneuous polynomials in x_1 of degree $\leq D$, and Bob's message space, $M_{Catherine}$ consists of homogeneuous polynomials in x_2 of degree $\leq D$ where $D \in \mathbb{N}$ is fixed.

Now, 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.

Before ending this section, we note that countermeasure 4.3 introduces an element of secret key encryption into the cryptosystem. However, it differs from traditional secret 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.

5. Conclusion

The chosen ciphertext attacks described in [2] and in this article are a matter of concern and should be taken into consideration in the design of a noncommutative polly cracker type cryptosystem. 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. Nor do they, as [2] suggests, render insecure, the simple examples that were presented in [7] and [9]. Rather, these attacks and the techniques to counter them, are small steps in an evolutionary process leading towards the development of a secure cryptosystem.

References

[1] P. Ackermann and M. Kreuzer, *Gröbner basis cryptosystems*, AAECC, 2005, to appear.

[2] S. Bulygin, *Chosen-ciphertext attack on noncommutative Polly Cracker*, Los Alamos XXX eprint archive, 0508015, 2005.

[3] R. Cramer, *An introduction to Crypto-Systems Secure Against Active Attacks* Lecture Notes, Part II of Cryptographic Protocol Theory (CPT), Comp. Sc. Dept. Aarhus University, Spring 2001.

[4] M. Fellows and N. Koblitz, *Combinatorial cryptosystems galore!* Contemporary Math. **168**, 1994, 51 - 61.

[5] L. Dickson, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors* Amer. J. Math., **35**, 1913, pp 413 - 426.

[6] E. L. Green, *Noncommutative Gröbner bases, and projective resolutions* Computational methods for representations of groups and algebras. Papers from the First Euroconference held at the University of Essen. Basel, 1999, P. Dräxler, G. O. Michler, and C. M. Ringel, Eds., no. **173** in Progress in Math., Birkhäuser Verlag, pp. 29-60.

[7] E. L. Green and T. Rai, *A public key cryptosystem based on noncommutative Gröbner bases* submitted.

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

[9] T. Rai, *Infinite Gröbner bases and noncommutative Polly Cracker cryptosystems* Ph.D. Dissertation, Virginia Tech, Blacksburg, VA, USA, 2004.

Department of Mathematics and Computer Science, University of Missouri - St. Louis, 303 CCB, One University Boulevard, St. Louis, MO 63121

E-mail address: rait@umsl.edu