Countering chosen-ciphertext attacks against noncomm. polly cracker cryptosystems.

Tapan S. Rai
University of Missouri - St. Louis
St. Louis, MO 63121, USA

and

Stanislav V. Bulygin
Technical University of Kaiserslautern
Kaiserslautern, Germany

Notation and Terminology

Definition 1 A well-order $>$ on a set of monomials, 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 $p \geq r$.

Let $f \in K\langle x_1, x_2, ..., x_n \rangle$, $B = \{\text{monomials}\}$, $supp\,(f) =$ support of f. Define tip$(f) =$ $\Big\{ b_i \in B : b_i \in supp\,(f)$ and $b_i \geq b_j \forall\ b_j \in supp\,(f) \Big\}$.

Denote the coefficient of tip(f) by Ctip(f).

If $X \subseteq R$, write

Tip(X) $= \{b \in B : b =$ tip(f) for some $f \in X\}$ and NonTip$(X) = B -$ Tip(X).

Gröbner Bases and Normal Forms

Definition 2 If $>$ is an admissible order on $R = K\langle x_1, x_2, \ldots, x_n\rangle$, 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 $\langle \text{Tip}(G)\rangle = \langle \text{Tip}(I)\rangle$.

Equivalently, $G \subset I$ is a Gröbner basis of I if for every $b \in \text{Tip}(I)$, there is some $g \in G$ such that $\text{tip}(g)$ divides b

i.e. for every $f \in I$, there exists $g \in G$, and $p, q \in B$ such that $p \cdot \text{tip}(g) \cdot q = \text{tip}(f)$.

Note: For any ideal I, $R = I \oplus \text{Span}(\text{NonTip}(I))$, as vector spaces.
In particular, every nonzero $r \in R$ can be written uniquely as $r = i_r + N_I(r)$,
where $i_r \in I$ and $N_I(r) \in \text{Span}(\text{NonTip}(I))$.
$N_I(r)$ is called the *normal form of r with respect to I*.

Reduced Gröbner Basis

Definition 3 Let I be an ideal in R, let T be the unique minimal monomial generating set of $\langle$Tip(I)$\rangle$. Then the *reduced Gröbner basis* for I, is $G = \{t - N(t) : t \in T\}$.

The following properites of min GB are clear:

1. G is a Gröbner basis for I.

2. If $g \in G$ then the coefficient of tip(g) is 1.

3. If $g_i, g_j \in G$ with $g_i \neq g_j$, and $b_i \in supp\,(g_i)$, then tip$\left(g_j\right) \not| \, b_i$.

4. If $g \in G$ then $g-$tip(g) $\in$ Span(NonTip(I)).

Note: Unlike the commutative case, the reduced Gröbner basis of an ideal may not be finite.

Some Ideals that do not have finite GB

1. (T. Mora, E. Green, V. Ufnarovski) Let g $= xyx - xy \in K\langle x, y\rangle$. Then $\langle g\rangle$ does not have a finite Gröbner basis under any admissible order.

2. Let $A \in K - \{0\}$ and let $g = xyx + Axz \in K\langle x, y, z\rangle$. Then $\langle g\rangle$ has an infinite reduced Gröbner basis under any admissible order in which $y \geq z$.

3. Let $g_1 = xzy + yz \in K\langle x, y, z\rangle$, $g_2 = yzx + zy \in K\langle x, y, z\rangle$. Then, $I = \langle g_1, g_2\rangle$ does not have a finite Gröbner basis under any admissible order.

Noncommutative polly cracker:

Private Key: A GB, $G = \{g_1, g_2, \ldots, g_t\}$ for a 2-sided ideal, I, of $K\langle x_1, x_2, ..., x_n\rangle$.

Public Key:
$Q = \left\{ q_r : q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij} \right\}_{r=1}^{s} \subset I$,

such that $\langle Q\rangle$ is computationally infeasible.
In practice, $\langle Q\rangle$ does not have a finite GB, and the GB of $\langle Q\rangle$ is not predictable.

Message Space: $M \subseteq$ NonTip(I) .

Encryption: $c = p + m$,

where $m \in M$ and

$p = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in J = \langle Q\rangle \subset I$.

$F_{rij}, H_{rij} \in K\langle x_1, x_2, ..., x_n\rangle$ are random.

Decryption: Reducing c modulo G yields m.

Some simple examples:

Example 4 *K a finite field, $R = K\langle x_1, x_2, \dots, x_6\rangle$.*

Let $Z = \prod_{i=1}^{6} x_i$ and $c_0, c_1, \dots, c_6 \in K - \{0\}$.

Private Key: *$g = Z + \sum_{i=1}^{6} c_i x_i + c_0 \in R$.*

Public Key: *$B = \{q_1, q_2\}$,*

where $q_1 = fgh + hg,\ q_2 = hgf + gh$,

$f = X + \sum_{i=1}^{6} a_i x_i + a_0,\ h = Y + \sum_{i=1}^{6} b_i x_i + b_0$,

$X = x_1 \cdot \prod_{i=2}^{5} \rho(x_i) \cdot x_6,\ Y = x_1 \cdot \prod_{i=2}^{5} \sigma(x_i) \cdot x_6$,

ρ, σ distinct permutations of $\{x_2, \dots x_5\}$,
$a_0, \dots, a_6, b_0, \dots, b_6 \in K - \{0\}$.

Message space: *M = linear polynomials in R.*

Alternatively, fix $D \in \mathbb{N}$. Then M = polynomials of degree $\leq D$ in some x_i.

Another Example

Example 5 *Let K be a finite field, $R = K\langle x, y\rangle$. Let $\alpha, \beta, \gamma, \delta \in K - \{0\}$.*

Private Key: *Set $g = \alpha xy + \beta x + \gamma y + \delta$ as the private key.*

Public Key: *For $i = 1 \ldots t$, set*
$f_i = a_i x^2 + b_i xy + c_i yx + d_i x + e_i y + u_i$,
$h_i = m_i y^2 + n_i x + k_i y + l_i$, *where*
$a_1, b_i, c_i, d_i, e_i, u_i, m_i, n_i, k_i, l_i \in K - \{0\}$
and $q_i = f_i g_i h_i$.
Then, $Q = \{q_1 \ldots q_t\}$ is the public key.

Message space: *M = linear polynomials in R.*

Alternatively, fix $D \in \mathbb{N}$. Then M = polynomials of degree $\leq D$ in some x_i.

The Attack

Definition 6 Let $f \in K\langle x_1, x_2, \ldots, x_n\rangle$. We define the *tail* of f by tail(f) $= f -$ Ctip(f) $\cdot$ tip(f).

Attack 7

<u>Assumptions:</u>

1. Alice's private key consists of a single polynomial, g, and tip(g) is publicly known.

2. Catherine, has temporary black box access to Alice's decryption algorithm.

Method:

1. Catherine "encrypts" tip(g). by constructing: $C = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} +$ tip(g).

2. She uses her temporary access to Alice's decryption black box to "decrypt" C.
   Note that $\sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle g \rangle$ vanishes, yielding
   $f = \text{tip}(g) - [\text{Ctip}(g)]^{-1} \cdot g = - [\text{Ctip}(g)]^{-1} \cdot \text{tail}(g)$.

3. 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 $\langle g \rangle$.

The Attack: Version 2

Attack 8

<u>Assumptions:</u>

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. Catherine has temporary black box access to Alice's decryption algorithm

Method:

1. Catherine encrypts tip(g_1). i.e. she creates ciphertext:
$C_1 = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + \text{tip}(\mathrm{g}_1)$.

2. She uses her temporary access to Alice's decryption black box to "decrypt" C_1.
Note that $\sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle G \rangle$ vanishes, yielding $f_1 = -\left[\text{Ctip}(g_1)\right]^{-1} \cdot \text{tail}(g_1)$.

3. Catherine constructs
$g_1' = \text{tip}(g_1) + \left[\text{Ctip}(g_1)\right]^{-1} \cdot \text{tail}(g_1)$.

4. By repeating this for $\alpha = 1, \ldots m$, she gets $G' = \left\{ g_1', \ldots g_m' \right\}$, where $g_\alpha' = \text{tip}(g_\alpha) + f_\alpha$.
Since $\text{Ctip}(g_\alpha) \cdot g_\alpha' = \text{Ctip}(g_\alpha) \cdot \text{tip}(g_\alpha) + \text{tail}(g_\alpha) = g_\alpha \; \forall \alpha = 1, 2, \ldots m$, it follows that $\langle G \rangle = \langle G' \rangle$, and that G' is a Gröbner basis for $\langle G \rangle$.

Generalizing the attack:

Attack 9

Assumptions:

1. Alice's private key consists of a finite 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 black box access to Alice's decryption algorithm.

Method:

1. Catherine encrypts tip(g_1) by constructing: $C_1 = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + \mathrm{tip(g_1)}$.

2. She uses her temporary access to Alice's decryption black box to "decrypt" C_1.

3. $\sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle G \rangle$ vanishes, and so does tip(g_1). In fact, the output of the decryption algorithm is $N_G(\mathrm{tip}(g_1))$.

4. Catherine constructs $g_1' = \text{tip}(g_1) - N_G(\text{tip}(g_1))$. Now, $g_1' = \text{tip}(g_1) - N_G(\text{tip}(g_1)) \in \langle G \rangle$.

5. She repeats this process for each $\alpha = 1, 2, \ldots m$, and obtains a set, $G' = \left\{g_1', g_2', \ldots g_m'\right\}$, where $g_\alpha' = \text{tip}(g_\alpha) - N_G(\text{tip}(g_\alpha))\ \forall \alpha = 1, 2, \ldots m$. Note that $g_\alpha' \in \langle G \rangle\ \forall \alpha = 1, 2, \ldots m$. i.e. $\langle G' \rangle \subset \langle G \rangle$. Furthermore, $\text{Tip}(G') = \text{Tip}(G)$.

6. It follows that $\langle G \rangle = \langle G' \rangle$, and that G' is a Gröbner basis for $\langle G \rangle$.

Generalized Attack: Version 2

Attack 10

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 black box access to Alice's decryption algorithm.

Method:

1. Catherine uses her knowledge of Alice's monomial order to determine the largest tip, T, that occurs in Alice's public key. Note that $T \in \langle \text{Tip}\,(G)\,\rangle$, and that $\text{tip}\,(g_i) \leq T \;\forall i = 1 \ldots m$.

2. Catherine encrypts T by constructing $C_T = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} + T$.

3. She uses her temporary access to Alice's decryption black box to "decrypt" C_T.

4. $\sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle G \rangle$ vanishes, and so does T. In fact, the output of the decryption algorithm yields $N_G\,(T)$.

5. Catherine constructs $g'_T = T - N_G(T)$. As noted earlier, $g'_T = T - N_G(T) \in \langle G \rangle$.

6. She repeats this process for each monomial b, such that $b \leq T$.

7. For each $b \leq T$, there are two possibilities: if $b \in \langle \mathsf{Tip}(G) \rangle$, then $N_G(b) \neq b$, and if $b \notin \langle \mathsf{Tip}(G) \rangle$, then $N_G(b) = b$.

8. If $b \in \langle \mathsf{Tip}(G) \rangle$, and $N_G(b)$, Catherine constructs $g'_b = b - N_G(b)$, and if $b \notin \langle \mathsf{Tip}(G) \rangle$, she discards b.

9. Since $\{b : b \leq T\}$ is finite, she obtains $G' = \left\{ g'_b = b - N_G(b) : b \leq T \text{ and } b \in \langle \mathsf{Tip}(G) \rangle \right\}$ in a finite number of steps.

10. Note that $g'_b \in \langle G \rangle \ \forall b$. i.e. $\langle G' \rangle \subset \langle G \rangle$. Furthermore, $\mathsf{Tip}(G) \subset \mathsf{Tip}\left(G'\right)$. So $\langle G \rangle = \langle G' \rangle$, and G' is a Gröbner basis for $\langle G \rangle$.

Countering the attack

Countermeasure 11

1. *Restrict the message space, M, so that* $\mathrm{NonTip}(G) - M \neq \emptyset$.

2. *For each each $g_i \in G$, ensure that $\exists b_i \in$ $supp\,(g_i)$, 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 for elements of* $\mathrm{NonTip}(G) - M$ *in the normal form of ciphertext polynomial after reduction modulo the private key.*

4. *If an element of* $\mathrm{NonTip}(G) - M$ *in the normal form of ciphertext, program it to return an error message.*

Some Examples

Example 12 *If $g = \alpha xy + \beta x + \gamma y + \delta$, as in example 5, 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.*

Example 13 *If $g = \prod_{i=1}^{6} x_i + \sum_{i=1}^{6} c_i x_i + c_0$, as in example 4 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.*

Why the countermeasure works:

1. Let $G = \{g_1, g_2, \ldots g_t\}$ be the private key. Let $m \notin M$ be a fake message let $C = p + m$.

2. Let $X_1 = u_1 \text{tip}\,(g_1)\, v_1$ for some $X_1 \in supp\,(C)$.

3. In the first step, C reduces to
$C_1 = C - A_X \cdot Ctip\,(g_1)^{-1} \cdot u_1 g_1 v_1$
$= A_X \cdot Ctip\,(g_1)^{-1}\,(u_1 \text{tip}\,(g_1)\, v_1 - u_1 \text{tail}\,(g_1)\, v_1)$,
where A_X is the coefficient of X in C.

4. $\exists b_1 \in supp\,(g_1)$ s.t. $b_1 \in \text{NonTip}(G) - M$, and $u \cdot b_1 \cdot v \notin M$. So, $u_1 \cdot b_1 \cdot v_1 \in supp\,(C_1)$, and $u_1 \cdot b_1 \cdot v_1 \notin M$.

5. If $\nexists g_i \in G$ such that $\text{tip}\,(g_i)$ divides some $X \in supp\,(C_1)$, 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.

6. If $\exists g_i \in G$ such that $\text{tip}(g_i)$ divides some $X \in supp(C_1)$, then the division proceeds 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.

7. Since G is a finite Gröbner basis, the division algorithm ends in a finite number of steps, yielding $N_G(C)$.

8. If $g_\nu \in G$ is the polynomial used in the final step of the division C by G, then $u_\nu b_\nu v_\nu$ occurs in $N_G(C)$, 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.

Adaptive chosen-ciphertext attacks

Attack 14 *(Koblitz)*

1. Suppose Bob encrypts a message m and sends it to Alice as ciphertext, c, and suppose Catherine is able to read c.

2. Catherine constructs $c' = p + c + m_0$, where $m_0 \in M$ is arbitrary. She sends c' to Alice.

3. She then informs Alice that an incomplete message was transmitted and requests her to send back the decrypted message $m' = N(c')$.

4. Since c' decrypts to $m' = m + m_0$, Catherine can find $m = m' - m_0$. Alice sees no connection between c' and c or m' and m.

Countermeasure

Countermeasure 15

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.

An Example

Example 16 *Suppose Alice chooses a private key based on example 4. i.e. suppose her private key consists of a single polynomial of the form* $g = x_1x_2x_3x_4x_5x_6 + \sum_{i=1}^{6} c_ix_i + c_0$.
She then implements countermeasure 11 by leaving all monomials that contain x_6 *out of her message space, thus securing her private key from attacks of that use illegitimate ciphertexts.*
Next she assigns the variable x_1 *to Bob and* x_2 *to Catherine.*
i.e. Bob's message space, M_{Bob} *consists of polynomials in* x_1 *of degree* $\leq D$,
and Catherine's message space, $M_{Catherine}$ *consists of polynomials in* x_2 *of degree* $\leq D$ *where* $D \in \mathbb{N}$ *is fixed.*

Why the countermeasure works

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.

Conclusion:

The noncommutative version of the Polly Cracker cryptosystem (and possibly also the commutative version) can be modified to resist chosen ciphertext attacks.