Lattice-based cryptography VI

Reaction attack on NTRU

Tanja Lange

Eindhoven University of Technology

SAC – Post-quantum cryptography

Reminder: decryption failures

Decryption of c wants that

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

has the integer factor 3 in the first part, even after reduction modulo q.
This works if the computed a equals $r \cdot 3g + f \cdot m$ in R, i.e., without reduction modulo q.
This works if everything is small enough compared to q.
For d non-zero coefficients in f and r the maximum coefficient of $r \cdot 3g + f \cdot m$ is

$$3d + d,$$

and typically much smaller.
Can choose q such that $q/2 > 4d$ – or hope for the best and expect coefficients not to collude.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.

$$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i \text{ has } a_I \in [-q/2, q/2].$$

(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + 1$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + f \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + f_i) x^i$$

which fails iff

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + 1$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + f \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + f_i) x^i$$

which fails iff $a_j = q/2$ and $f_j = 1$.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c - 1$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m - f \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i - f_i) x^i$$

which fails iff

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c - 1$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m - f \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i - f_i) x^i$$

which fails iff $a_j = q/2$ and $f_j = -1$.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + x$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + fx \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + f_{i-1}) x^i$$

which fails iff
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + x$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + fx \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + f_{i-1}) x^i$$

which fails iff $a_j = q/2$ and $f_{j-1} = 1$.
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + x^k$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + fx^k \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + f_{i-k}) x^i$$

which fails iff
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + x^k$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + fx^k \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + f_{i-k}) x^i$$

which fails iff $a_j = q/2$ and $f_{j-k} = 1$.
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + 2x^k$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + 2fx^k \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + 2f_{i-k}) x^i$$

which fails iff
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + 2x^k$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + 2fx^k \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + 2f_{i-k}) x^i$$

which fails iff $a_j = q/2 - 1$ and $f_{j-k} = 1$.
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + \ell x^k$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + \ell f x^k \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + \ell f_{i-k}) x^i$$

which fails iff
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + \ell x^k$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + \ell f x^k \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + \ell f_{i-k}) x^i$$

which fails iff $a_j = q/2 - \ell + 1$ and $f_{j-k} = 1$.
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.

How to craft input for a reaction attack?

$$a = f \cdot c = r \cdot 3g + f \cdot m \bmod q,$$

Assume that c is such that a decrypts correctly, i.e.
$a = r \cdot 3g + f \cdot m = \sum_{i=0}^{n-1} a_i x^i$ has $a_I \in [-q/2, q/2]$.
(You can test this with a reaction attack.)
Assume for some j that $|a_j| > |a_i|$ for $i \neq j$ and assume that $a_j > 0$.

Sending $c' = c + \ell x^k$ leads to

$$a' = f \cdot c' = r \cdot 3g + f \cdot m + \ell f x^k \bmod q,$$

thus

$$a' = \sum_{i=0}^{n-1} (a_i + \ell f_{i-k}) x^i$$

which fails iff $a_j = q/2 - \ell + 1$ and $f_{j-k} = 1$.
Remember that in R computations happen modulo $x^n - 1$,
thus indices of f are taken modulo n.
Try all k, then increase ℓ. Once the first failure happens, get all coefficients of f with ℓ and $-\ell$, running through $0 \leq k < n$.

Better attacks fewer assumptions

- Full attack without assumptions, see Jeffrey Hoffstein, Joseph H. Silverman: Reaction Attacks Against the NTRU Public Key Cryptosystem (NTRU Tech Report #015v2, 2000) for this attack and unconditional version.
- More general reaction attack, also against other lattice-based systems exist.
  See Scott R. Fluhrer: Cryptanalysis of ring-LWE based key exchange with key share reuse, 2016. IACR Cryptology ePrint Archive 2016/085.