Lattice-based cryptography IV

NTRU

Tanja Lange
(with some slides from Daniel J. Bersntein and Nadia Heninger)

Eindhoven University of Technology

SAC – Post-quantum cryptography

NTRU history

- Introduced by Hoffstein, Pipher, and Silverman in 1996.
- Presented as an alternative to RSA and ECC;
  higher speed but larger key size & ciphertext.
- Good amount of research into attacks during last 20 years.
    - NTRU signature scheme had a bit of a bumpy ride.

NTRU history

- Introduced by Hoffstein, Pipher, and Silverman in 1996.
- Presented as an alternative to RSA and ECC;
  higher speed but larger key size & ciphertext.
- Good amount of research into attacks during last 20 years.
  - NTRU signature scheme had a bit of a bumpy ride.
  - NTRU encryption held up after first change of parameters.
- Far less research into efficient implementation and secure usage

NTRU history

- Introduced by Hoffstein, Pipher, and Silverman in 1996.
- Presented as an alternative to RSA and ECC;
  higher speed but larger key size & ciphertext.
- Good amount of research into attacks during last 20 years.
  - NTRU signature scheme had a bit of a bumpy ride.
  - NTRU encryption held up after first change of parameters.
- Far less research into efficient implementation and secure usage
  – why invest research effort into patented scheme...
- NTRU patent finally expired now.

For code snippets to try things yourself see
https://latticehacks.cr.yp.to/.

NTRU operations

NTRU works with polynomials over the integers of degree less than some system parameter $250 < n < 2500$.

$$R = \mathbf{Z}[x]/(x^n - 1).$$

We add component wise

$$\sum_{i=0}^{n-1} a_i x^i + \sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^{n-1} (a_i + b_i) x^i.$$

Note that multiplication in R is fast because reductions modulo $x^n - 1$ are easy.

$$(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}) \cdot (b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1}) =$$
$$(a_0 b_0 + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-1} b_1) +$$
$$(a_0 b_1 + a_1 b_0 + a_2 b_{n-1} + \cdots + a_{n-1} b_2) x + \cdots +$$
$$(a_0 b_{n-1} + a_1 b_{n-2} + a_2 b_{n-3} + \cdots + a_{n-1} b_0) x^{n-1}$$

This operation is also called *cyclic convolution*.

More NTRU parameters

- NTRU specifies integer n (as above).
- Integer q, typically a power of 2.
  In any case, q must not be multiple of 3.
- Some computations work in $R_q = (\mathbf{Z}/q)[x]/(x^n - 1)$,
  meaning we reduce the coefficients of the polynomials modulo q.
- Same for modulo 3.

More NTRU parameters

- NTRU specifies integer n (as above).
- Integer q, typically a power of 2.
  In any case, q must not be multiple of 3.
- Some computations work in $R_q = (\mathbf{Z}/q)[x]/(x^n - 1)$,
  meaning we reduce the coefficients of the polynomials modulo q.
- Same for modulo 3.
- Pick $f, g \in R$ with coefficients in $\{-1, 0, 1\}$, almost all coefficients are zero (f and g have t coefficients equal to 1, f has $t - 1$ coefficients equal to -1 and g has g coefficients equal to -1).
- Public key $h \in R$ with $h \cdot f = 3g \bmod q$.
  If no such h exists, start over with new f.
- In math notation $h = 3g/f \bmod q$ in $\mathbf{Z}[x]/(x^n - 1)$.
  Note that this requires $f(1) \neq 0$.
- Private key f and f_3 with $f \cdot f_3 = 1 \bmod 3$.

NTRU encryption (schoolbook version)

- Public key $h \in R$ with $h \cdot f = 3g \bmod q$.
- Encryption of message $m \in R$, coefficients in $\{-1, 0, 1\}$:
  - Pick random $r \in R$, with coefficients in $\{-1, 0, 1\}$, almost all coefficients are zero
    (same conditions as g).
  - Compute
    $$c = r \cdot h + m \bmod q.$$
  - Send ciphertext c.
- Decryption of $c \in R_q$:
  - Compute
    $$a = f \cdot c = f \cdot (r \cdot h + m) = r \cdot 3g + f \cdot m \bmod q$$
    using $h \cdot f = 3g \bmod q$.
  - Move all coefficients of a to $[-q/2, q/2]$.
  - If everything is small enough then a equals $r \cdot 3g + f \cdot m$ in R and
    $$m = a \cdot f_3 \bmod 3,$$
    using $f \cdot f_3 = 1 \bmod 3$.

Problem!

Problem!

$$((11 \bmod 3) \bmod 2) = 0 \text{ but } ((11 \bmod 2) \bmod 3) = 1.$$

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.

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.

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.

NTRU – translation to lattices

- Public key h with $h \cdot f = 3g \bmod q$.
- Can see this as lattice with basis matrix

$$B = \begin{pmatrix} q\,I_n & 0 \\ H & I_n \end{pmatrix},$$

  where H corresponds to multiplication $\cdot$ by $h/3$ in R.
- So

$$((1,0,0,\ldots,0),(3,0,0,\ldots,0)) \begin{pmatrix} q\,I_n & 0 \\ H & I_n \end{pmatrix}$$
$$= ((q,0,0,\ldots,0)+(h_0,h_1,\ldots,h_{n-1}),(3,0,0,\ldots,0))).$$

NTRU – translation to lattices

- Public key h with $h \cdot f = 3g \bmod q$.
- Can see this as lattice with basis matrix

$$B = \begin{pmatrix} q\, I_n & 0 \\ H & I_n \end{pmatrix},$$

  where H corresponds to multiplication $\cdot$ by $h/3$ in R.
- So

$$((1,0,0,\ldots,0),(3,0,0,\ldots,0)) \begin{pmatrix} q\, I_n & 0 \\ H & I_n \end{pmatrix}$$
$$= ((q,0,0,\ldots,0) + (h_0,h_1,\ldots,h_{n-1}),(3,0,0,\ldots,0))).$$

- (g,f) is a short vector in the lattice as result of

$$(-k,f)B = (-kq + f \cdot h/3, f) = (g,f)$$

  for some $k \in R$ (from $h \cdot f = 3g \bmod q$, i.e., $h \cdot f = 3g + 3kq$).

NTRU – translation to lattices

- Public key h with $h \cdot f = 3g \bmod q$.
- Can see this as lattice with basis matrix

$$B = \begin{pmatrix} q\, I_n & 0 \\ H & I_n \end{pmatrix},$$

  where H corresponds to multiplication $\cdot$ by $h/3$ in R.
- So

$$((1,0,0,\ldots,0),(3,0,0,\ldots,0)) \begin{pmatrix} q\, I_n & 0 \\ H & I_n \end{pmatrix} = ((q,0,0,\ldots,0)+(h_0,h_1,\ldots,h_{n-1}),(3,0,0,\ldots,0))).$$

- (g, f) is a short vector in the lattice as result of

$$(-k, f)B = (-kq + f \cdot h/3, f) = (g, f)$$

  for some $k \in R$ (from $h \cdot f = 3g \bmod q$, i.e., $h \cdot f = 3g + 3kq$).
- Note that the attack need not find (g, f), any reasonably short (g', f') works for decryption.