Solving Bézout Equations using the Field Norm and Applications to NTRU

Thomas Pornin / Thomas Prest

NCC Group / Thales

The NTRU equation

Let $\mathcal{Z}_n = \mathbb{Z}[x]/(x^n+1)$ – or $\mathcal{Z}$ when n is clear from context. Given two polynomials $f, g \in \mathcal{Z}$, we want to find $F, G \in \mathcal{Z}$ such that:

$$f \times G - g \times F = 1 \bmod (x^n + 1) \tag{1}$$

We call this the NTRU equation.

Let $\mathcal{C}(f)$ be the $n \times n$-matrix which i-th row is the coefficients of $x^i f \bmod (x^n+1)$. The NTRU equation is equivalent to

$$\left[\ \mathcal{C}(G) \mid -\mathcal{C}(F)\ \right] \times \left[\frac{\mathcal{C}(f)}{\mathcal{C}(g)}\right] = I_n \tag{2}$$

The NTRU equation

Let $\mathcal{Z}_n = \mathbb{Z}[x]/(x^n + 1)$ – or $\mathcal{Z}$ when n is clear from context. Given two polynomials $f, g \in \mathcal{Z}$, we want to find $F, G \in \mathcal{Z}$ such that:

$$f \times G - g \times F = 1 \bmod (x^n + 1) \quad (1)$$

We call this the NTRU equation.

Let $\mathcal{C}(f)$ be the $n \times n$-matrix which i-th row is the coefficients of $x^i f \bmod (x^n + 1)$. The NTRU equation is equivalent to

$$\left[\ \mathcal{C}(G) \ \middle|\ -\mathcal{C}(F)\ \right] \times \left[\frac{\mathcal{C}(f)}{\mathcal{C}(g)}\right] = I_n \quad (2)$$

Solving an NTRU equation is part of the key generation in:

- Stehlé-Steinfeld's provably secure NTRUSign [SS11]
- Ducas-Lyubashevsky-Prest's IBE [DLP14]
- The Falcon signature scheme [Pre+17]
- Also, LATTE [CG17] entails solving a very similar equation

Easy to solve in time $O(n \log n)$ over $\{\mathbb{R}, \mathbb{Z}_q\}[x]/(x^n + 1)$, not so much over $\mathcal{Z}_n$!

The Classical Solvers

The Classical Solvers

Two previous methods:

- A number theoretic one, proposed in [Hof+03] and used in e.g. [DLP14]
- A method based on the Hermite normal form, proposed in [SS11]

Both are extremely costly in time and memory, hard to implement.

Number Theoretic Method

Algorithm 1 Number theoretic NTRU-solver

Require: $f, g \in \mathcal{Z}$
Ensure: $F, G \in \mathcal{Z}$ such that $fG - gF = 1$
1: Using ext. Euclid, find $\rho_f \in \mathcal{Z}$ and $R_f \in \mathbb{Z}$ such that $\rho_f \times f = R_f$
2: Using ext. Euclid, find $\rho_g \in \mathcal{Z}$ and $R_g \in \mathbb{Z}$ such that $\rho_g \times g = R_g$
3: Using ext. Euclid, find $\alpha, \beta \in \mathbb{Z}$ such that $\alpha R_f + \beta R_g = 1$
4: $G \leftarrow \alpha \rho_f$
5: $F \leftarrow -\beta \rho_g$
6: Reduce (F, G) with respect to (f, g)

A few remarks:

- Steps 1, 2, 3 might fail, in which case we abort the algorithm.
- At the end of step 5, the equation 1 is solved, but the solution (F, G) is huge.
- Step 6 is a Babai round-off reduction of (F, G) with respect to (f, g).

Number Theoretic Method

Algorithm 1 Number theoretic NTRU-solver

Require: $f, g \in \mathcal{Z}$
Ensure: $F, G \in \mathcal{Z}$ such that $fG - gF = 1$
1: Using ext. Euclid, find $\rho_f \in \mathcal{Z}$ and $R_f \in \mathbb{Z}$ such that $\rho_f \times f = R_f$
2: Using ext. Euclid, find $\rho_g \in \mathcal{Z}$ and $R_g \in \mathbb{Z}$ such that $\rho_g \times g = R_g$
3: Using ext. Euclid, find $\alpha, \beta \in \mathbb{Z}$ such that $\alpha R_f + \beta R_g = 1$
4: $G \leftarrow \alpha \rho_f$
5: $F \leftarrow -\beta \rho_g$
6: Reduce (F, G) with respect to (f, g)

About the size:

- $R_f = \text{Res}(f, x^n + 1) = \det(\mathcal{C}(f))$ may be as large as $\|f\|_2^n$ (same remark applies to R_g and $\|g\|_2^n$).
- Each coefficient of ρ_f, ρ_g may be as large as $\|f\|_2^n$, $\|g\|_2^n$.
- Each coefficient of F, G may be as large as $\|f\|_2^n \times \|g\|_2^n$.

Number Theoretic Method: Example in Sage

```
sage: f
-x^7 + 3*x^6 - x^4 + 4*x^3 + 6*x^2 - 2*x - 4
sage: g
x^7 - x^6 - 2*x^5 - 4*x^3 - 3*x^2 - x + 7
sage: rho_f
-124199*x^7 - 870168*x^6 - 289656*x^5 - 766237*x^4 + 643331*
    x^3 - 1336173*x^2 + 708821*x - 1082620
sage: rho_g
665170*x^7 + 1421014*x^6 + 2065365*x^5 - 2640*x^4 + 1213571*
    x^3 + 682454*x^2 - 648356*x + 3666911
sage: F
3409956090310*x^7 + 7284747273202*x^6 + 10587975946695*x^5 -
     13533809520*x^4 + 6221302557953*x^3 + 3498561531122*x^2
     - 3323760077708*x + 18798210227573
sage: G
-1882599996468*x^7 - 13189947372576*x^6 - 4390585951392*x^5
    - 11614568341884*x^4 + 9751567551492*x^3 -
    20253619474236*x^2 + 10744260518172*x - 16410280341840
```

HNF Method

Given $M \in \mathbb{Z}^{m \times n}$, the Hermite Normal Form (or HNF) of M consists of finding $U \in \mathbb{Z}^{n \times m}, H \in \mathbb{Z}^{n \times n}$ such that:

1. $U \times M = H$,
2. U is unimodular,
3. H is upper triangular.

Algorithm 2 HNF NTRU-solver

Require: $f, g \in \mathcal{Z}$

Ensure: $F, G \in \mathcal{Z}$ such that $fG - gF = 1$

1: $M \leftarrow \left[\frac{\mathcal{C}(f)}{\mathcal{C}(g)}\right]$

2: $U, H \leftarrow \text{HNF}(M)$[1]

3: $G \leftarrow \sum_{i=0}^{n-1} u_{0,i} x^i$, $F \leftarrow -\sum_{i=0}^{n-1} u_{0,i+n} x^i$

4: Reduce (F, G) with respect to (f, g)

5: **return** (F, G)

---

[1] From my experiments, either $H = I_n$ or the NTRU equation has no solution for (f, g).

HNF Method: Example in Sage

```
sage: f
-x^7 + 3*x^6 - x^4 + 4*x^3 + 6*x^2 - 2*x - 4
sage: g
x^7 - x^6 - 2*x^5 - 4*x^3 - 3*x^2 - x + 7
sage: M
[-4 -2  6  4 -1  0  3 -1]
[ 1 -4 -2  6  4 -1  0  3]
[-3  1 -4 -2  6  4 -1  0]
[ 0 -3  1 -4 -2  6  4 -1]
[ 1  0 -3  1 -4 -2  6  4]
[-4  1  0 -3  1 -4 -2  6]
[-6 -4  1  0 -3  1 -4 -2]
[ 2 -6 -4  1  0 -3  1 -4]
[-----------------------]
[ 7 -1 -3 -4  0 -2 -1  1]
[-1  7 -1 -3 -4  0 -2 -1]
[ 1 -1  7 -1 -3 -4  0 -2]
[ 2  1 -1  7 -1 -3 -4  0]
[ 0  2  1 -1  7 -1 -3 -4]
[ 4  0  2  1 -1  7 -1 -3]
[ 3  4  0  2  1 -1  7 -1]
[ 1  3  4  0  2  1 -1  7]
sage: U
[0  0  0  0  0  0  0   1448400   -520289   698444   -33146   -230429    62160   204165   1814   1115570]
[0  0  0  0  0  0  0  39291927 -14114306 18947260  -899179  -6251036  1686265  5538549  49209  30262976]
[0  0  0  0  0  0  0  12999110  -4669494  6268400  -297479  -2068056   557874  1832341  16280  10012025]
[0  0  0  0  0  0  0  22532034  -8093877 10865344  -515636  -3584669   966992  3176092  28219  17354364]
[0  0  0  0  0  0  0  41515695 -14913120 20019600  -950069  -6604820  1781701  5852009  51994  31975741]
[0  0  0  0  0  0  0  24008442  -8624227 11577294  -549423  -3819554  1030354  3384205  30068  18491506]
[0  0  0  0  0  0  0  39651209 -14243366 19120512  -907401  -6308195  1701684  5589193  49659  30539698]
[0  0  0  0  0  0  0  32866681 -11806252 15848893  -752140  -5228830  1410517  4632853  41162  25314197]
sage: U*M == identity_matrix(ZZ,8)
True
sage: F
-1115570*x^7 - 1814*x^6 - 204165*x^5 - 62160*x^4 + 230429*x^3 + 33146*x^2 - 698444*x + 520289
sage: G
1448400*x^7
```

A New Solver based on Towers of Rings

Exploiting the tower of rings structure

We have the following tower of rings:

$$\mathbb{Z} \subseteq \mathbb{Z}[x]/(x^2+1) \subseteq \cdots \subseteq \mathbb{Z}[x]/(x^{n/2}+1) \subseteq \mathbb{Z}[x]/(x^n+1)$$

and the field norm allows to "navigate" along this tower!

Let $\mathcal{Q}_n = \mathbb{Q}[x]/(x^n+1)$. The field norm N is defined by:

$$\begin{array}{cccc} \mathrm{N} & : & \mathcal{Q}_n & \to & \mathcal{Q}_{n/2} \\ & & f & \to & f f^{\times} \end{array} \quad (3)$$

where in our case $f^{\times}(x) = f(-x)$.

Fun fact: if we have this relationship over $\mathbb{Z}[x]/(x^{n/2}+1)$:

$$\mathrm{N}(f)G' - \mathrm{N}(g)F' = 1 \quad (4)$$

for some F', G', then we have this relationship over $\mathbb{Z}[x]/(x^n+1)$:

$$f(f^{\times}G') - g(g^{\times}F') = 1 \quad (5)$$

Outline of the new solver

$$
\begin{array}{ccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g \\
\cup\!\wr & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & & \\
\cup\!\wr & & \\
\mathbb{Z}[x]/(x^{n/4}+1) & & \\
\cup\!\wr & & \\
\vdots & & \\
\cup\!\wr & & \\
\mathbb{Z} & &
\end{array}
\tag{6}
$$

Outline of the new solver

$$\begin{array}{ccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g \\
\cup\!\!\wr & & \downarrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f), \mathsf{N}(g) \\
\cup\!\!\wr & & \\
\mathbb{Z}[x]/(x^{n/4}+1) & & \\
\cup\!\!\wr & & \\
\vdots & & \\
\cup\!\!\wr & & \\
\mathbb{Z} & &
\end{array} \tag{6}$$

Outline of the new solver

$$
\begin{array}{ccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g \\
\cup\!\wr & & \downarrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f), \mathsf{N}(g) \\
\cup\!\wr & & \downarrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathsf{N}^2(f), \mathsf{N}^2(g) \\
\cup\!\wr & & \\
\vdots & & \\
\cup\!\wr & & \\
\mathbb{Z} & &
\end{array}
\tag{6}
$$

Outline of the new solver

$$
\begin{array}{ccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g \\
\cup\!\wr & & \downarrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f), \mathsf{N}(g) \\
\cup\!\wr & & \downarrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathsf{N}^2(f), \mathsf{N}^2(g) \\
\cup\!\wr & & \downarrow \\
\vdots & \vdots & \vdots \\
\cup\!\wr & & \\
\mathbb{Z} & &
\end{array}
\tag{6}
$$

Outline of the new solver

$$
\begin{array}{ccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g \\
\cup\shortmid & & \downarrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) \\
\cup\shortmid & & \downarrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) \\
\cup\shortmid & & \downarrow \\
\vdots & \vdots & \vdots \\
\cup\shortmid & & \downarrow \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f), \mathrm{N}^\ell(g)
\end{array}
\tag{6}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & & \\
\cup\!\!\!\!\nmid & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f), \mathsf{N}(g) & & \\
\cup\!\!\!\!\nmid & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathsf{N}^2(f), \mathsf{N}^2(g) & & \\
\cup\!\!\!\!\nmid & & \downarrow & & \\
\vdots & \vdots & \vdots & & \\
\cup\!\!\!\!\nmid & & \downarrow & & \\
\mathbb{Z} & \ni & \mathsf{N}^\ell(f), \mathsf{N}^\ell(g) & \to & F^{[\ell]}, G^{[\ell]}
\end{array}
\tag{6}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & & \\
\cup & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f), \mathsf{N}(g) & & \\
\cup & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathsf{N}^2(f), \mathsf{N}^2(g) & & \\
\cup & & \downarrow & & \\
\vdots & \vdots & \vdots & & \vdots \\
\cup & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathsf{N}^\ell(f), \mathsf{N}^\ell(g) & \to & F^{[\ell]}, G^{[\ell]}
\end{array}
\tag{6}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & & \\
\cup & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f), \mathsf{N}(g) & & \\
\cup & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathsf{N}^2(f), \mathsf{N}^2(g) & \rightarrow & F^{[2]}, G^{[2]} \\
\cup & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\cup & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathsf{N}^{\ell}(f), \mathsf{N}^{\ell}(g) & \rightarrow & F^{[\ell]}, G^{[\ell]}
\end{array}
\tag{6}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & & \\
\cup\!\!\! \nmid & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) & \to & F^{[1]}, G^{[1]} \\
\cup\!\!\! \nmid & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) & \to & F^{[2]}, G^{[2]} \\
\cup\!\!\! \nmid & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\cup\!\!\! \nmid & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f), \mathrm{N}^\ell(g) & \to & F^{[\ell]}, G^{[\ell]}
\end{array} \tag{6}
$$

Outline of the new solver

$$\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & \to & F, G \\
\cup\!\!\restriction & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f), \mathsf{N}(g) & \to & F^{[1]}, G^{[1]} \\
\cup\!\!\restriction & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathsf{N}^2(f), \mathsf{N}^2(g) & \to & F^{[2]}, G^{[2]} \\
\cup\!\!\restriction & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\cup\!\!\restriction & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathsf{N}^\ell(f), \mathsf{N}^\ell(g) & \to & F^{[\ell]}, G^{[\ell]}
\end{array} \tag{6}$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f,g & \rightarrow & F,G \\
\cup\!\wr & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f),\mathrm{N}(g) & \rightarrow & F^{[1]},G^{[1]} \\
\cup\!\wr & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f),\mathrm{N}^2(g) & \rightarrow & F^{[2]},G^{[2]} \\
\cup\!\wr & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\cup\!\wr & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f),\mathrm{N}^\ell(g) & \rightarrow & F^{[\ell]},G^{[\ell]}
\end{array}
\tag{6}
$$

At each lower level:

- The coefficients grow (in bitsize) by a factor 2...
- ... but the number of coefficients is divided by 2.

Space-saving trick: recompute lazily $\mathrm{N}^i(f), \mathrm{N}^i(g)$ at each step

- Allows a linear time-memory trade-off by a factor $\ell = \log n$

The recursive variant (fast)

Algorithm 3 TowerSolverR$_{n,q}(f, g)$

Require: $f, g \in \mathbb{Z}[x]/(x^n + 1)$ with n a power of two

Ensure: Polynomials F, G such that the equation 1 is verified

```
if n = 1 then
    Compute u, v ∈ ℤ such that uf − vg = 1
    (F, G) ← (v, u)
    return (F, G)
else
    f′ ← N(f)                                  ▷ f′, g′, F′, G′ ∈ ℤ[x]/(x^{n/2} + 1)
    g′ ← N(g)
    (F′, G′) ← TowerSolverR_{n/2,q}(f′, g′)
    F ← g^×(x)F′(x²)                           ▷ F, G ∈ ℤ[x]/(x^n + 1)
    G ← f^×(x)G′(x²)
    Reduce (F, G) with respect to (f, g)
return (F, G)
```

The iterative variant (compact but slower)

Algorithm 4 TowerSolverI$_{n,q}(f, g)$

Require: $f, g \in \mathbb{Z}[x]/(x^n + 1)$ with n a power of two
Ensure: Polynomials F, G such that the equation 1 is verified

```
(f′, g′) ← (f, g)
for i ← 1, ..., log n do
    (f′, g′) ← (N(f′), N(g′))
Compute u, v ∈ ℤ such that uf′ − vg′ = 1
(F, G) ← (v, u)
for i ← log n, ..., 1 do
    (f′, g′) ← (f, g)
    for j ← 1, ..., i − 1 do
        (f′, g′) ← (N(f′), N(g′))
    (F, G) ← (g′^× F, f′^× G)
    Reduce (F, G) with respect to (f′, g′)
return (F, G)
```

```
sage: f8, g8
-x^7 + 3*x^6 - x^4 + 4*x^3 + 6*x^2 - 2*x - 4,
x^7 - x^6 - 2*x^5 - 4*x^3 - 3*x^2 - x + 7
sage: f4, g4
-51*x^3 + 51*x^2 - 54*x - 17, -33*x^3 - 4*x^2 - 47*x + 57
sage: f2, g2
-2049*x + 3196, -1576*x + 6335
sage: f1, g1
14412817, 42616001
sage: F1, G1
5126443, 15157932
sage: F2, G2
2495*x - 399, 3844*x - 2025
sage: F4, G4
-22*x^3 + 39*x^2 - 23*x - 14, -x^3 - 45*x + 5
sage: F8, G8
-x^7 - x^5 + 3*x^4 + 3*x^3 - 3*x^2 + 4,
2*x^7 - x^6 - x^5 - x^4 - 3*x^3 + x^2 + x - 4
```

Performances

Method	**Time complexity**	**Space complexity**
Resultant [Hof+03]	$\tilde{O}(n(n^2 + B))$	$O(n^2 B)$
HNF [SS11]	$\tilde{O}(n^3 B)$	$O(n^2 B)$
This work (Fast)	$O((nB)^{\log_2 3} \log n)$ [Kara] $\tilde{O}(nB)$ [SchöStr]	$O(n(B + \log n) \log n)$
This work (Compact)	$O((nB)^{\log_2 3} \log^2 n)$ [Kara] $\tilde{O}(nB)$ [SchöStr]	$O(n(B + \log n) \log n)$

We gain in practice:

- a factor 100 in memory (3 MB $\to$ 30 kB)
- a factor 100 in time (2 sec. $\to$ 20 msec.)

Corollary: also allows to compute $\text{Res}(f, x^n + 1)$ faster and with less memory.

Open problems

Open problems:

1. Get rid of large integers:
   - By adequate use of the CRT?
2. Reduce memory consumption further:
   - Doesn't seem trivial: the value $\mathrm{N}_{\backslash\mathbb{Q}}(f)$ is an invariant of the algorithm;
3. Combine with classical methods (+ the one in appendix)?
4. Similar applications of the field norm (constructive of destructive)?

Point 1 and 2 are probably connected, but maybe not.

Thanks!

Peter Campbell and Michael Groves. *Practical Post-Quantum Hierarchical Identity-Based Encryption*. 16th IMA International Conference on Cryptography and Coding. http://www.qub.ac.uk/sites/CSIT/FileStore/Filetoupload,785752,en.pdf. 2017.

Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. "Efficient Identity-Based Encryption over NTRU Lattices". In: *ASIACRYPT 2014, Part II*. Ed. by Palash Sarkar and Tetsu Iwata. Vol. 8874. LNCS. Springer, Heidelberg, Dec. 2014, pp. 22–41. doi: 10.1007/978-3-662-45608-8_2.

Jeffrey Hoffstein et al. "NTRUSIGN: Digital Signatures Using the NTRU Lattice". In: *CT-RSA 2003*. Ed. by Marc Joye. Vol. 2612. LNCS. Springer, Heidelberg, Apr. 2003, pp. 122–140. doi: 10.1007/3-540-36563-X_9.

Thomas Prest et al. *FALCON*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions. National Institute of Standards and Technology, 2017.

Damien Stehlé and Ron Steinfeld. "Making NTRU as Secure as Worst-Case Problems over Ideal Lattices". In: *EUROCRYPT 2011*. Ed. by Kenneth G. Paterson. Vol. 6632. LNCS. Springer, Heidelberg, May 2011, pp. 27–47. doi: 10.1007/978-3-642-20465-4_4.