More Efficient Algorithms for the NTRU Key Generation using the Field Norm

Thomas Pornin / Thomas Prest

NCC Group / PQShield

Motivation

NTRU Lattices:

- Prevalent in lattice-based crypto
- Public key is $\mathbf{A} = \left[\begin{array}{c|c} 1 & h \end{array}\right]$, for $h = g \times f^{-1} \bmod (\varphi, q)$.
- Private key is $\mathbf{B}$ such that $\mathbf{B} \times \mathbf{A}^t = 0 \bmod (\varphi, q)$

Some schemes only require a partial trapdoor $\mathbf{B} = \left[\begin{array}{c|c} g & -f \end{array}\right]$:

- Fiat-Shamir [Zha+17], encryption [Sch+17], FHE [LTV12; Bos+13]

Motivation

NTRU Lattices:

- Prevalent in lattice-based crypto
- Public key is $\mathbf{A} = \left[\begin{array}{c|c} 1 & h \end{array}\right]$, for $h = g \times f^{-1} \bmod (\varphi, q)$.
- Private key is $\mathbf{B}$ such that $\mathbf{B} \times \mathbf{A}^t = 0 \bmod (\varphi, q)$

Some schemes only require a partial trapdoor $\mathbf{B} = \left[\begin{array}{c|c} g & -f \end{array}\right]$:

- Fiat-Shamir [Zha+17], encryption [Sch+17], FHE [LTV12; Bos+13]

However, some schemes require a full trapdoor $\mathbf{B} = \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array}\right]$:

- Hash-then-sign [Pre+17], IBE [DLP14], HIBE [CG17]
- More generally, anything based on trapdoor sampling [GPV08]

Motivation

NTRU Lattices:

- Prevalent in lattice-based crypto
- Public key is $\mathbf{A} = \left[\begin{array}{c|c} 1 & h \end{array}\right]$, for $h = g \times f^{-1} \bmod (\varphi, q)$.
- Private key is $\mathbf{B}$ such that $\mathbf{B} \times \mathbf{A}^t = 0 \bmod (\varphi, q)$

Some schemes only require a partial trapdoor $\mathbf{B} = \left[\begin{array}{c|c} g & -f \end{array}\right]$:

- Fiat-Shamir [Zha+17], encryption [Sch+17], FHE [LTV12; Bos+13]

However, some schemes require a full trapdoor $\mathbf{B} = \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array}\right]$:

- Hash-then-sign [Pre+17], IBE [DLP14], HIBE [CG17]
- More generally, anything based on trapdoor sampling [GPV08]

Given $f, g \in \mathbb{Z}[x]/(x^n + 1)$, we want to find $F, G \in \mathbb{Z}[x]/(x^n + 1)$ such that:

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

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

The Classical Solvers

The Classical Solvers

Two previous methods:

- A method based on resultants, 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.

Resultant-Based Method

Algorithm 1 Resultant-based NTRU-solver

Require: $f, g \in \mathbb{Z}[x]/(\varphi)$
Ensure: $F, G \in \mathbb{Z}[x]/(\varphi)$ such that $fG - gF = 1$

1: Using ext. Euclid, find $\rho_f \in \mathbb{Z}[x]/(\varphi)$ and $R_f \in \mathbb{Z}$ such that $\rho_f \times f = R_f$
2: Using ext. Euclid, find $\rho_g \in \mathbb{Z}[x]/(\varphi)$ 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).
- Completely agnostic to the structure of the ring $\mathbb{Z}[x]/(\varphi)$.

Resultant-Based Method

Algorithm 1 Resultant-based NTRU-solver

Require: $f, g \in \mathbb{Z}[x]/(\varphi)$
Ensure: $F, G \in \mathbb{Z}[x]/(\varphi)$ such that $fG - gF = 1$

1: Using ext. Euclid, find $\rho_f \in \mathbb{Z}[x]/(\varphi)$ and $R_f \in \mathbb{Z}$ such that $\rho_f \times f = R_f$
2: Using ext. Euclid, find $\rho_g \in \mathbb{Z}[x]/(\varphi)$ 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:

- $R_f = \mathrm{Res}(f, \varphi) = \det(\mathcal{C}(f))$ 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 $\|f\|_2^n \times \|g\|_2^n$.

Resultant-Based 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 + 728474727320 2*x^6 + 1058975946695*x^5 -
     13533809520*x^4 + 622130255795 3*x^3 + 349856153112 2*x^2
     - 332376007770 8*x + 1879821022757 3
sage: G
-1882599996468*x^7 - 1318994737257 6*x^6 - 439058595139 2*x^5
    - 116145683418 84*x^4 + 97515675514 92*x^3 -
    202536194742 36*x^2 + 107442605181 72*x - 164102803418 40
```

The State of Affairs

- Existing methods are slow ($O(n^3)$) and take space $O(n^2)$
- Existing methods consider the underlying ring as a black-box
- What happens when we open this black box?

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 (w.r.t. the extension $\mathcal{Q}_n/\mathcal{Q}_{n/2}$) is defined by:

$$\begin{array}{ccccc} \mathsf{N} & : & \mathcal{Q}_n & \rightarrow & \mathcal{Q}_{n/2} \\ & & f & \rightarrow & ff^{\times} \end{array} \tag{2}$$

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

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

$$\mathsf{N}(f)G' - \mathsf{N}(g)F' = 1 \tag{3}$$

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

$$f(f^{\times}G') - g(g^{\times}F') = 1 \tag{4}$$

Outline of the new solver

$$\begin{array}{ccc} \mathbb{Z}[x]/(x^n+1) & \ni & f, g \\ \cup\!\!\!\!\!\!\backslash \\ \mathbb{Z}[x]/(x^{n/2}+1) \\ \cup\!\!\!\!\!\!\backslash \\ \mathbb{Z}[x]/(x^{n/4}+1) \\ \cup\!\!\!\!\!\!\backslash \\ \vdots \\ \cup\!\!\!\!\!\!\backslash \\ \mathbb{Z} \end{array} \tag{5}$$

Outline of the new solver

$$\begin{array}{ccc} \mathbb{Z}[x]/(x^n+1) & \ni & f, g \\ \cup\!\!\!\!\!\!\backslash & & \downarrow \\ \mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f), \mathsf{N}(g) \\ \cup\!\!\!\!\!\!\backslash & & \\ \mathbb{Z}[x]/(x^{n/4}+1) & & \\ \cup\!\!\!\!\!\!\backslash & & \\ \vdots & & \\ \cup\!\!\!\!\!\!\backslash & & \\ \mathbb{Z} & & \end{array} \tag{5}$$

Outline of the new solver

$$
\begin{array}{ccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g \\
\cup\!\!\!\!\backslash & & \downarrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) \\
\cup\!\!\!\!\backslash & & \downarrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) \\
\cup\!\!\!\!\backslash & & \\
\vdots & & \\
\cup\!\!\!\!\backslash & & \\
\mathbb{Z} & &
\end{array}
\tag{5}
$$

Outline of the new solver

$$
\begin{array}{ccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g \\
\cup\!\!\!\!\!\!\backslash & & \downarrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) \\
\cup\!\!\!\!\!\!\backslash & & \downarrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) \\
\cup\!\!\!\!\!\!\backslash & & \downarrow \\
\vdots & \vdots & \vdots \\
\cup\!\!\!\!\!\!\backslash & & \\
\mathbb{Z} & &
\end{array}
\tag{5}
$$

Outline of the new solver

$$
\begin{array}{ccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g \\
\cup\!\!\!\!\!\!\backslash & & \downarrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) \\
\cup\!\!\!\!\!\!\backslash & & \downarrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) \\
\cup\!\!\!\!\!\!\backslash & & \downarrow \\
\vdots & \vdots & \vdots \\
\cup\!\!\!\!\!\!\backslash & & \downarrow \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f), \mathrm{N}^\ell(g)
\end{array}
\tag{5}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & & \\
\cup\!\!\upharpoonleft & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) & & \\
\cup\!\!\upharpoonleft & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) & & \\
\cup\!\!\upharpoonleft & & \downarrow & & \\
\vdots & \vdots & \vdots & & \\
\cup\!\!\upharpoonleft & & \downarrow & & \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f), \mathrm{N}^\ell(g) & \rightarrow & F^{[\ell]}, G^{[\ell]}
\end{array}
\tag{5}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & & \\
\cup\!\!\!\!\!\!\backslash & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) & & \\
\cup\!\!\!\!\!\!\backslash & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) & & \\
\cup\!\!\!\!\!\!\backslash & & \downarrow & & \\
\vdots & \vdots & \vdots & & \vdots \\
\cup\!\!\!\!\!\!\backslash & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f), \mathrm{N}^\ell(g) & \rightarrow & F^{[\ell]}, G^{[\ell]}
\end{array}
\tag{5}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & & \\
\cup\!\!\upharpoonleft & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) & & \\
\cup\!\!\upharpoonleft & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) & \rightarrow & F^{[2]}, G^{[2]} \\
\cup\!\!\upharpoonleft & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\cup\!\!\upharpoonleft & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f), \mathrm{N}^\ell(g) & \rightarrow & F^{[\ell]}, G^{[\ell]}
\end{array}
\tag{5}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & & \\
\cup\!\!\downarrow & & \downarrow & & \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) & \rightarrow & F^{[1]}, G^{[1]} \\
\cup\!\!\downarrow & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) & \rightarrow & F^{[2]}, G^{[2]} \\
\cup\!\!\downarrow & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\cup\!\!\downarrow & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f), \mathrm{N}^\ell(g) & \rightarrow & F^{[\ell]}, G^{[\ell]}
\end{array}
\tag{5}
$$

Outline of the new solver

$$
\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f, g & \to & F, G \\
\cup\!\!\upharpoonleft & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathrm{N}(f), \mathrm{N}(g) & \to & F^{[1]}, G^{[1]} \\
\cup\!\!\upharpoonleft & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathrm{N}^2(f), \mathrm{N}^2(g) & \to & F^{[2]}, G^{[2]} \\
\cup\!\!\upharpoonleft & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\cup\!\!\upharpoonleft & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathrm{N}^\ell(f), \mathrm{N}^\ell(g) & \to & F^{[\ell]}, G^{[\ell]}
\end{array}
\tag{5}
$$

Outline of the new solver

$$\begin{array}{ccccc}
\mathbb{Z}[x]/(x^n+1) & \ni & f,g & \to & F,G \\
\cup\!\!\upharpoonright & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/2}+1) & \ni & \mathsf{N}(f),\mathsf{N}(g) & \to & F^{[1]},G^{[1]} \\
\cup\!\!\upharpoonright & & \downarrow & & \uparrow \\
\mathbb{Z}[x]/(x^{n/4}+1) & \ni & \mathsf{N}^2(f),\mathsf{N}^2(g) & \to & F^{[2]},G^{[2]} \\
\cup\!\!\upharpoonright & & \downarrow & & \uparrow \\
\vdots & \vdots & \vdots & & \vdots \\
\cup\!\!\upharpoonright & & \downarrow & & \uparrow \\
\mathbb{Z} & \ni & \mathsf{N}^\ell(f),\mathsf{N}^\ell(g) & \to & F^{[\ell]},G^{[\ell]}
\end{array} \tag{5}$$

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 $\mathsf{N}^i(f),\mathsf{N}^i(g)$ at each step

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

The recursive variant (fast)

Algorithm 1 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 $u, v \in \mathbb{Z}$ such that $uf - vg = 1$
    $(F, G) \leftarrow (v, u)$
    return (F, G)
else
    $f' \leftarrow \mathrm{N}(f)$ ▷ $f', g', F', G' \in \mathbb{Z}[x]/(x^{n/2} + 1)$
    $g' \leftarrow \mathrm{N}(g)$
    $(F', G') \leftarrow$ TowerSolverR$_{n/2,q}(f', g')$
    $F \leftarrow g^{\times}(x)F'(x^2)$ ▷ $F, G \in \mathbb{Z}[x]/(x^n + 1)$
    $G \leftarrow f^{\times}(x)G'(x^2)$
    Reduce (F, G) with respect to (f, g)
return (F, G)

The iterative variant (compact but slower)

Algorithm 2 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

$(f', g') \leftarrow (f, g)$
for $i \leftarrow 1, \ldots, \log n$ **do**
    $(f', g') \leftarrow (\mathrm{N}(f'), \mathrm{N}(g'))$
Compute $u, v \in \mathbb{Z}$ such that $uf' - vg' = 1$
$(F, G) \leftarrow (v, u)$
for $i \leftarrow \log n, \ldots, 1$ **do**
    $(f', g') \leftarrow (f, g)$
    for $j \leftarrow 1, \ldots, i - 1$ **do**
        $(f', g') \leftarrow (\mathrm{N}(f'), \mathrm{N}(g'))$
    $(F, G) \leftarrow (g'^{\times} F, f'^{\times} G)$
    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**[1]	**Space complexity**[1]
Resultant [Hof+03]	$\tilde{O}(n(n^2+B))$	$O(n^2B)$
HNF [SS11]	$\tilde{O}(n^3B)$	$O(n^2B)$
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]	$O(n(B+\log n))$

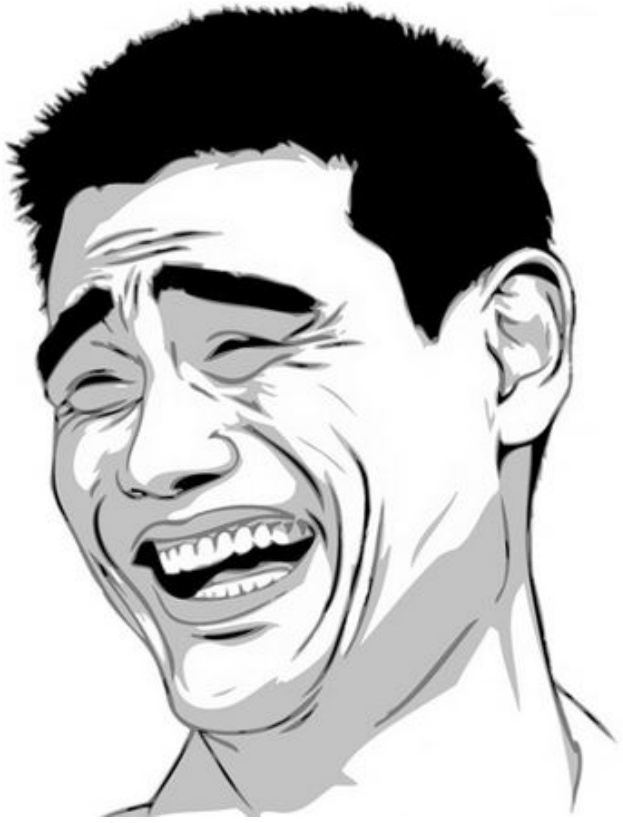
We gain in practice:

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

[1] $B = \log_2 ||(f,g)||$

Key takeaway

If you cannot trivially exploit the presence of a ring...



... try to use its particular structure!

Thanks!

Joppe W. Bos et al. "Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme". In: *14th IMA International Conference on Cryptography and Coding*. Ed. by Martijn Stam. Vol. 8308. LNCS. Springer, Heidelberg, Dec. 2013, pp. 45–64. DOI: 10.1007/978-3-642-45239-0_4.

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.

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". In: *40th ACM STOC*. Ed. by Richard E. Ladner and Cynthia Dwork. ACM Press, May 2008, pp. 197–206. DOI: 10.1145/1374376.1374407.

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.

Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption". In: *44th ACM STOC*. Ed. by Howard J. Karloff and Toniann Pitassi. ACM Press, May 2012, pp. 1219–1234. DOI: 10.1145/2213977.2214086.

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.

John M. Schanck et al. *NTRU-HRSS-KEM*. 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.

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