# NTWE: A Natural Combination of NTRU and LWE

Joel Gärtner

KTH Royal Institute of Technology

August 16, 2023

# NTWE Problem

- Introduce NTWE problem as a natural combination of the NTRU and LWE problems

# NTWE Problem

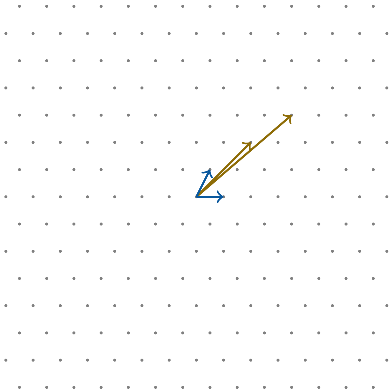
- Introduce NTWE problem as a natural combination of the NTRU and LWE problems
- Consider both the provable and concrete hardness of NTWE problem

# NTWE Problem

- Introduce NTWE problem as a natural combination of the NTRU and LWE problems
- Consider both the provable and concrete hardness of NTWE problem
- Construct and parametrize a NTWE-based cryptosystem

# Lattice-Based Cryptography

- Primary candidate for post-quantum cryptography
- Lattice-based KEM and signature algorithm to be standardized by NIST



# Assumptions in Lattice-Based Cryptography

- Primary two building blocks are NTRU [HPS98] and LWE [Reg05] problems
- Interesting to investigate alternative hardness assumptions
- We introduce the NTWE problem as a new problem for lattice-based cryptography

# Problem Statements

- Use ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ with integers $n, q$
- Typical parameters $q = 3329$, $n = 256$ and $k < 5$

### Module-LWE $\mathrm{MLWE}(k)$

Distinguish between uniformly random $(\overline{\boldsymbol{A}} \in R_q^{m \times k}, \overline{\boldsymbol{b}} \in R_q^m)$ and $(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = \overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})$ with uniformly random $\overline{\boldsymbol{A}}$ and small $\overline{\boldsymbol{s}} \in R_q^k$, $\overline{\boldsymbol{e}} \in R_q^m$

# Problem Statements

- Use ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ with integers $n, q$
- Typical parameters $q = 3329$, $n = 256$ and $k < 5$

### Module-LWE $\mathrm{MLWE}(k)$

Distinguish between uniformly random $(\overline{\boldsymbol{A}} \in R_q^{m\times k}, \overline{\boldsymbol{b}} \in R_q^m)$ and $(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = \overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})$ with uniformly random $\overline{\boldsymbol{A}}$ and small $\overline{\boldsymbol{s}} \in R_q^k$, $\overline{\boldsymbol{e}} \in R_q^m$

### NTRU

Distinguish between uniformly random $h \in R_q$ and $h = gf^{-1}$ for small $g, f \in R_q$

# Problem Statements

- Use ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ with integers $n, q$
- Typical parameters $q = 3329$, $n = 256$ and $k < 5$

**Module-LWE $\mathrm{MLWE}(k)$**

Distinguish between uniformly random $(\overline{\boldsymbol{A}} \in R_q^{m \times k}, \overline{\boldsymbol{b}} \in R_q^m)$ and $(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = \overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})$ with uniformly random $\overline{\boldsymbol{A}}$ and small $\overline{\boldsymbol{s}} \in R_q^k$, $\overline{\boldsymbol{e}} \in R_q^m$

**Module NTRU $\mathrm{MNTRU}(k)$**

Distinguish between uniformly random $\overline{\boldsymbol{H}} \in R_q^{m \times k}$ and $\overline{\boldsymbol{H}} = \overline{\boldsymbol{G}}\overline{\boldsymbol{F}}^{-1}$ and small $\overline{\boldsymbol{G}} \in R_q^{m \times k}, \overline{\boldsymbol{F}} \in R_q^{k \times k}$

# Problem Statements

- Use ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ with integers $n, q$
- Typical parameters $q = 3329$, $n = 256$ and $k < 5$

### Module-LWE $\mathrm{MLWE}(k)$

Distinguish between uniformly random $(\overline{\boldsymbol{A}} \in R_q^{m \times k}, \overline{\boldsymbol{b}} \in R_q^m)$ and $(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = \overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})$ with uniformly random $\overline{\boldsymbol{A}}$ and small $\overline{\boldsymbol{s}} \in R_q^k$, $\overline{\boldsymbol{e}} \in R_q^m$

### Module NTRU $\mathrm{MNTRU}(k)$

Distinguish between uniformly random $\overline{\boldsymbol{H}} \in R_q^{m \times k}$ and $\overline{\boldsymbol{H}} = \overline{\boldsymbol{G}\boldsymbol{F}}^{-1}$ and small $\overline{\boldsymbol{G}} \in R_q^{m \times k}, \overline{\boldsymbol{F}} \in R_q^{k \times k}$

### NTWE Problem $\mathrm{NTWE}(k)$

Distinguish between uniformly random $(\overline{\boldsymbol{A}} \in R_q^{m \times k}, \overline{\boldsymbol{b}} \in R_q^m)$ and $(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = (\overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})f^{-1})$ with uniformly random $\overline{\boldsymbol{A}}$, small $\overline{\boldsymbol{e}} \in R_q^m$, $\overline{\boldsymbol{s}} \in R_q^k$ and $f \in R_q$

# Problem Hardness

## Provable Hardness

- NTWE problem a natural combination of NTRU and LWE problems
- Can easily see that the NTWE problem is not easier than either of these problems

# Problem Hardness

## Provable Hardness

- NTWE problem a natural combination of NTRU and LWE problems
- Can easily see that the NTWE problem is not easier than either of these problems

## Concrete Hardness

- NTWE problem naturally corresponds to a lattice problem
- The hardness of this lattice problem gives a concrete hardness estimate for the NTWE problem

# Provable Relation to MLWE problem

- Given $\mathrm{MLWE}(k)$ instance $\overline{\boldsymbol{A}} \in \mathbb{R}_q^{m \times k}, \overline{\boldsymbol{b}} \in \mathbb{R}_q^m$
- Sample $f$ from correct distribution and $(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} \cdot f^{-1})$ is an $\mathrm{NTWE}(k)$ instance
- Solving $\mathrm{NTWE}(k)$ instance gives solution to original $\mathrm{MLWE}(k)$ instance

# Provable Relation to NTRU Problem

- Given NTRU instance with multiple samples $h_i = g_i f^{-1}$
- Sample $\boldsymbol{A}$ uniformly at random and produce NTWE instance with

$$\boldsymbol{b} = \boldsymbol{A}\boldsymbol{h}_{[1,\dots,k]} + \boldsymbol{h}_{[k+1,\dots k+m]} \left(\boldsymbol{A}\boldsymbol{g}_{[1,\dots,k]} + \boldsymbol{g}_{[k+1,\dots k+m]}\right) \cdot f^{-1}$$

- Solving NTWE instance implies solution to original NTRU instance

# Reduction From More Structured NTWE to MNTRU Problem

- More structured variant of $\mathrm{NTWE}(k)$ is at least as hard as $\mathrm{MNTRU}(k+1)$
- Additional structure might make the NTWE problem harder
- More natural to assume that less structure corresponds to harder problems

# Concrete Hardness of NTWE Problem

- NTWE corresponds to problem of finding unusually short vector in a lattice

**NTWE($k$) Lattice**

Lattice given by $\boldsymbol{A} \in \mathbb{Z}_q^{mn \times kn}$, $\boldsymbol{B} \in \mathbb{Z}_q^{mn \times n}$

# Concrete Hardness of NTWE Problem

- NTWE corresponds to problem of finding unusually short vector in a lattice
- $\mathrm{NTWE}(k)$ with $\boldsymbol{H} = \boldsymbol{A} \parallel \boldsymbol{B}$ gives same type of lattice as $\mathrm{MNTRU}(k+1)$

**$\mathrm{NTWE}(k)$ Lattice**

Lattice given by $\boldsymbol{A} \in \mathbb{Z}_q^{mn \times kn}$, $\boldsymbol{B} \in \mathbb{Z}_q^{mn \times n}$

**$\mathrm{MNTRU}(k+1)$ Lattice**

Lattice given by $\boldsymbol{H} \in \mathbb{Z}_q^{mn \times (k+1)n}$

# Concrete Hardness of NTWE Problem

- NTWE corresponds to problem of finding unusually short vector in a lattice
- $\mathrm{NTWE}(k)$ with $\boldsymbol{H} = \boldsymbol{A} \parallel \boldsymbol{B}$ gives same type of lattice as $\mathrm{MNTRU}(k+1)$
- $\mathrm{NTWE}(k)$ lattice very similar to $\mathrm{MLWE}(k+1)$ lattice

**$\mathrm{NTWE}(k)$ Lattice**

Lattice given by $\boldsymbol{A} \in \mathbb{Z}_q^{mn \times kn}$, $\boldsymbol{B} \in \mathbb{Z}_q^{mn \times n}$

**$\mathrm{MNTRU}(k+1)$ Lattice**

Lattice given by $\boldsymbol{H} \in \mathbb{Z}_q^{mn \times (k+1)n}$

**$\mathrm{MLWE}(k+1)$ Lattice**

Lattice given by $\boldsymbol{A} \in \mathbb{Z}_q^{mn \times (k+1)n}$, $\boldsymbol{b} \in \mathbb{Z}_q^{mn \times 1}$

# Concrete Hardness of NTWE Problem

- NTWE corresponds to problem of finding unusually short vector in a lattice
- $\mathrm{NTWE}(k)$ with $\boldsymbol{H} = \boldsymbol{A} \parallel \boldsymbol{B}$ gives same type of lattice as $\mathrm{MNTRU}(k+1)$
- $\mathrm{NTWE}(k)$ lattice very similar to $\mathrm{MLWE}(k+1)$ lattice
- Concrete hardness of these types of lattice problems is well studied [CN11, Che13, APS15, ACD$^+$18]

**$\mathrm{NTWE}(k)$ Lattice**

Lattice given by $\boldsymbol{A} \in \mathbb{Z}_q^{mn \times kn}$, $\boldsymbol{B} \in \mathbb{Z}_q^{mn \times n}$

**$\mathrm{MNTRU}(k+1)$ Lattice**

Lattice given by $\boldsymbol{H} \in \mathbb{Z}_q^{mn \times (k+1)n}$

**$\mathrm{MLWE}(k+1)$ Lattice**

Lattice given by $\boldsymbol{A} \in \mathbb{Z}_q^{mn \times (k+1)n}$, $\boldsymbol{b} \in \mathbb{Z}_q^{mn \times 1}$

# NTWE-Based Cryptosystem

Alice → Bob: $(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = (\overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})f^{-1})$

Bob → Alice: $c_1 = \overline{\boldsymbol{s}}' \cdot \overline{\boldsymbol{b}} + e' + \lfloor Mq/2 \rceil$, $\overline{\boldsymbol{c}}_2 = \overline{\boldsymbol{s}}' \cdot \overline{\boldsymbol{A}} + \overline{\boldsymbol{e}}''$

$$M = \lfloor 2(c_1 f - \overline{\boldsymbol{c}}_2 \cdot \overline{\boldsymbol{s}})/q \rceil \cdot f_2^{-1}$$

## Cryptosystem Construction

- Use public matrix $\overline{\boldsymbol{A}} \in R_q^{k \times (k-1)}$
- Ciphertext is $k$ samples from $\mathrm{MLWE}(k)$ instance
- Decryption correct as products of $\overline{\boldsymbol{s}}, \overline{\boldsymbol{e}}, f, \overline{\boldsymbol{s}}', e', \overline{\boldsymbol{e}}''$ small

# Comparable MLWE-Based Cryptosystem

Alice | Bob

$(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = \overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})$ $\longrightarrow$

$\longleftarrow$ $c_1 = \overline{\boldsymbol{s}}' \cdot \overline{\boldsymbol{b}} + e' + \lfloor Mq/2 \rceil$

$\overline{\boldsymbol{c}}_2 = \overline{\boldsymbol{s}}' \cdot \overline{\boldsymbol{A}} + \overline{\boldsymbol{e}}''$

$$M = \lfloor 2(c_1 - \overline{\boldsymbol{c}}_2 \cdot \overline{\boldsymbol{s}})/q \rceil$$

## Cryptosystem Construction

- Public matrix $\overline{\boldsymbol{A}} \in R_q^{k \times k}$
- Ciphertext is $k+1$ samples from $\mathrm{MLWE}(k)$ instance
- Decryption correct as products of $\overline{\boldsymbol{s}}, \overline{\boldsymbol{e}}, \overline{\boldsymbol{s}}', \overline{\boldsymbol{e}}''$ and $e'$ small

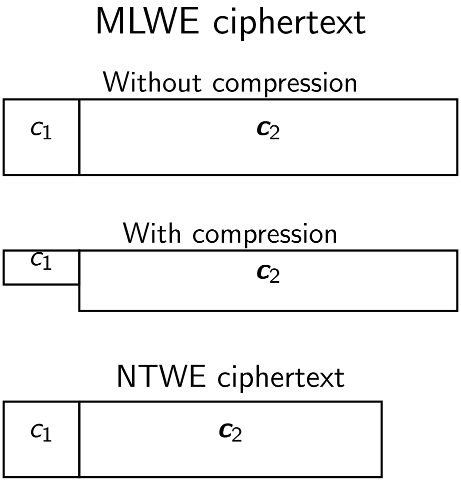
# Parametrizations of NTWE-Based Cryptosystem

- Parametrizations with same ring $R = \mathbb{Z}[X]/(X^{256} + 1)$ and modulos $q = 3329$ as in Kyber [SAB+22]
- Similar distributions for $\overline{\boldsymbol{s}}$ and $\overline{\boldsymbol{e}}$ as in Kyber
- More efficient than Kyber as requires fewer operations of equivalent cost

| Version | NTWE-768 | Kyber-768 | NTWE-1024 | Kyber-1024 |
|---|---|---|---|---|
| Core SVP | 182 | 183 | 256 | 256 |
| Dimension of $\overline{\boldsymbol{A}}$ | $3 \times 2$ | $3 \times 3$ | $4 \times 3$ | $4 \times 4$ |
| PK size (bytes) | 1184 | 1184 | 1568 | 1568 |
| CT size (bytes) | 1152 | 1088 | 1536 | 1568 |
| $\delta$ | $2^{-182}$ | $2^{-164}$ | $2^{-153}$ | $2^{-174}$ |

# Ciphertext Compression

- MLWE-based cryptosystems use ciphertext compression to allow for smaller ciphertexts
- Ciphertext compression not suitable for all applications
- NTWE-based cryptosystem without ciphertext compression allows more efficient encryption and decryption



# Efficiency of Operations

- Multiplication, inversion and addition in $R_q$ efficient with NTT
- Multiplication and inversion in $R_2$ during decryption
  less efficient as not performed with
- Sampling $f$ such that it is trivial in $R_2$ ensures no operations in $R_2$ are required

Alice | Bob

$$(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = (\overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}}) f^{-1}) \longrightarrow$$

$$(\overline{\boldsymbol{A}}, \overline{\boldsymbol{b}} = \overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})$$

$$\longleftarrow c_1 = \overline{\boldsymbol{s}}' \cdot \overline{\boldsymbol{b}} + e' + \lfloor Mq/2 \rceil$$

$$\overline{\boldsymbol{c}}_2 = \overline{\boldsymbol{s}}' \cdot \overline{\boldsymbol{A}} + \overline{\boldsymbol{e}}''$$

$$M = \lfloor 2(c_1 f - \overline{\boldsymbol{c}}_2 \cdot \overline{\boldsymbol{s}})/q \rceil f_2^{-1}$$

$$M = \lfloor 2(c_1 - \overline{\boldsymbol{c}}_2 \cdot \overline{\boldsymbol{s}})/q \rceil$$

# Efficiency of Operations

- Multiplication, inversion and addition in $R_q$ efficient with NTT
- Multiplication and inversion in $R_2$ during decryption
  less efficient as not performed with
- Sampling $f$ such that it is trivial in $R_2$ ensures no operations in $R_2$ are required

Alice — Bob

$$\text{Alice} \xrightarrow[(\overline{\boldsymbol{A}},\, \overline{\boldsymbol{b}} = \overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}})]{(\overline{\boldsymbol{A}},\, \overline{\boldsymbol{b}} = (\overline{\boldsymbol{A}} \cdot \overline{\boldsymbol{s}} + \overline{\boldsymbol{e}}) f^{-1})} \text{Bob}$$

$$\text{Alice} \xleftarrow[\overline{\boldsymbol{c}}_2 = \overline{\boldsymbol{s}}' \cdot \overline{\boldsymbol{A}} + \overline{\boldsymbol{e}}'']{c_1 = \overline{\boldsymbol{s}}' \cdot \overline{\boldsymbol{b}} + e' + \lfloor Mq/2 \rceil} \text{Bob}$$

$$M = \lfloor 2(c_1 f - \overline{\boldsymbol{c}}_2 \cdot \overline{\boldsymbol{s}})/q \rceil$$

$$M = \lfloor 2(c_1 - \overline{\boldsymbol{c}}_2 \cdot \overline{\boldsymbol{s}})/q \rceil$$

# Conclusion

- Introduced the NTWE problem with provable relations to NTRU and LWE problems

# Conclusion

- Introduced the NTWE problem with provable relations to NTRU and LWE problems
- Estimated the concrete hardness of the NTWE problem based on the hardness of the natural corresponding lattice problem

# Conclusion

- Introduced the NTWE problem with provable relations to NTRU and LWE problems
- Estimated the concrete hardness of the NTWE problem based on the hardness of the natural corresponding lattice problem
- Constructed a NTWE-based cryptosystem with performance competitive with highly efficient lattice-based cryptosystems

Questions?

Martin R. Albrecht, Benjamin R. Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W. Postlethwaite, Fernando Virdia, and Thomas Wunderer.
Estimate all the LWE, NTRU schemes!
pages 351–367, 2018.

Martin R. Albrecht, Rachel Player, and Sam Scott.
On the concrete hardness of learning with errors.
Cryptology ePrint Archive, Report 2015/046, 2015.
https://eprint.iacr.org/2015/046.

Yuanmi Chen.
*Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe*.
PhD thesis, Université Paris Diderot, 2013.
2013PA077242.

Yuanmi Chen and Phong Q. Nguyen.
BKZ 2.0: Better lattice security estimates.
pages 1–20, 2011.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.

NTRU: A ring-based public key cryptosystem.
In *Third Algorithmic Number Theory Symposium (ANTS)*, volume 1423, pages 267–288, June 1998.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
pages 84–93, 2005.

Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding.
CRYSTALS-KYBER.
Technical report, National Institute of Standards and Technology, 2022.
available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`.