

NTRU+

Jonghyun Kim

Korea University
yoswuk@korea.ac.kr

Februray 25, 2026

Outline

- NTRU+ Construction
 - NTRU and correctness issue
 - Fixing the correctness issue
 - Final NTRU+
- Ring Operations
 - Ring decomposition
 - Number Theoretic Transform
 - Base multiplication
 - Base inversion
- Resources

NTRU+ Construction

Overview of NTRU+

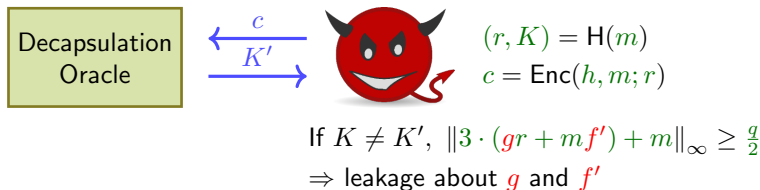
- NTRU-type KEM over an NTT-friendly ring
 - $R_q = \mathbb{Z}_q[x] / \langle x^n - x^{n/2} + 1 \rangle$
- Simple distribution: centered binomial distribution (CBD)
 - $\psi_1 : b_0 - b_1 \in \{-1, 0, 1\}$ with $b_0, b_1 \leftarrow \{0, 1\}$
- Compact parameters with negligible worst-case correctness error
- IND-CCA security without re-encryption
- Parameter sets: NTRU+768, NTRU+864, NTRU+1152

GenNTRU[ψ_1^n]: A Variant of Classical NTRU

- $\text{Gen}(1^\lambda)$
 - $sk = f = 3f' + 1, \quad pk = h = 3gf^{-1} \in R_q$
 - sample $f', g \leftarrow \psi_1^n$ until f is invertible in R_q
- $\text{Enc}(pk, m \in \{-1, 0, 1\}^n)$
 - $c = hr + m \in R_q$
 - $r \leftarrow \psi_1^n$
- $\text{Dec}(sk, c)$
 - $m = (cf \bmod^\pm q) \bmod^\pm 3$
- Correctness condition
 - $\|3(gr + mf') + m\|_\infty < q/2 \Rightarrow$ depends on the message m

Correctness Issue in the CCA Setting

- In the FO transformation:
 - An adversary can choose m to trigger decryption failure
 - $r = H(m)$ is hash-derived and not directly controllable
 - Decryption failure may leak information about the secret key



Green: known to adversary Red: secret information

Fixing the Correctness Issue

- How do we prevent adversarially induced decryption failures?
- Solution 1 - perfect correctness
 - No (m, r) pair causes decryption failure
 - Requires larger modulus q and/or fixed-weight (m, r)
- Solution 2 - negligible worst-case correctness error
 - Encrypt $M = \text{Encode}(m, r)$ instead of m
 - M remains honestly distributed (r is hash-derived)
 - Proposed in NTRU-B [2], refined in NTRU+ [4]

Semi-generalized OTP (SOTP)

- $\text{Encode}(m, u)$
 - $m \in \{0, 1\}^n$
 - $u = (u_0, u_1) \in \{0, 1\}^n \times \{0, 1\}^n$
 - return $y = (m \oplus u_0) - u_1$

$$y \sim \psi_1^n \text{ if } u_0, u_1 \leftarrow \{0, 1\}^n$$

- $\text{Decode}(y, u)$
 - $u = (u_0, u_1) \in \{0, 1\}^n \times \{0, 1\}^n$
 - If $y + u_1 \notin \{0, 1\}^n$, return \perp
 - return $m = (y + u_1) \oplus u_0$

$$\text{PKE}' = \text{ACWC}_2[\text{GenNTRU}[\psi_1^n], \text{SOTP}, G]$$

- $\text{Enc}'(pk, m \in \mathcal{M}', r \leftarrow \psi_1^n)$
 - $M = \text{Encode}(m, G(r))$
 - $c = \text{Enc}(pk, M; r)$
 - $c = hr + M$
 - return c
- $\text{Dec}'(sk, c)$
 - $M = \text{Dec}(sk, c)$
 - $r = \text{RRec}(pk, M, c)$
 - $r = (c - M)h^{-1}$
 - $m = \text{Decode}(M, G(r))$
 - If $m = \perp$ or $r \notin \mathcal{R}$, return \perp
 - return m

FO without Re-encryption

- $\text{Encap}(pk)$
 - $m \leftarrow \{0, 1\}^n$
 - $(K, r) \leftarrow H(m)$
 - $c = \text{Enc}'(pk, m; r)$
 - $M = \text{Encode}(m, G(r))$
 - $c = \text{Enc}(pk, M; r)$
 - return (c, K)
- $\text{Decap}(sk, c)$
 - $m = \text{Dec}'(sk, c)$
 - $M = \text{Dec}(sk, c)$
 - $r = \text{RRec}(pk, M, c)$
 - $m = \text{Decode}(M, G(r))$
 - $(K, r') = H(m)$
 - If $c = \text{Enc}'(pk, m; r')$, $r \in \mathcal{R}$, $r = r'$, and $m \neq \perp$
 - return K
 - Else, return \perp

Final NTRU+

- $\text{Gen}(1^\lambda)$
 - $f' \leftarrow \psi_1^n$ until $f = 3f' + 1$ is invertible
 - $g' \leftarrow \psi_1^n$ until $g = 3g'$ is invertible
 - $pk = h = gf^{-1}$
 - $sk = (f, h^{-1}, F(pk))$
 - return (pk, sk)
- $\text{Encap}(pk)$
 - $m \leftarrow \{0, 1\}^n$
 - $(K, R) \leftarrow H(m, F(pk))$
 - $r \leftarrow \psi_1^n$ with randomness R
 - $M \leftarrow \text{Encode}(m, G(r))$
 - $c = hr + M$
 - return (c, K)
- $\text{Decap}(sk, c)$
 - $M = (cf \bmod^\pm q) \bmod^\pm 3$
 - $r = (c - M)h^{-1}$
 - $m \leftarrow \text{Decode}(M, G(r))$
 - $(K, R) \leftarrow H(m, F(pk))$
 - $r' \leftarrow \psi_1^n$ with randomness R
 - If $m = \perp$ or $r \neq r'$, return \perp
 - Else, return K

Reference Code Structure

- kem.c
 - crypto_kem_keypair
 - crypto_kem_enc
 - crypto_kem_dec
- symmetric.c
 - hash_f, hash_g, hash_h
- poly.c
 - poly_tobytes, poly_frombytes
 - poly_cbd1, poly_sotp_encode, poly_sotp_decode
 - poly_ntt, poly_invntt
 - poly_baseinv, poly_basemul, poly_basemul_add
 - poly_sub, poly_triple, poly_crepmod3
- ntt.c
 - ntt, invntt
 - baseinv, basemul, basemul_add

Ring Operations

The Ring Structure of NTRU+

- NTRU+ is defined over the cyclotomic ring

$$R_q = \mathbb{Z}_q[x] / \langle x^n - x^{n/2} + 1 \rangle, \quad n = 2^a 3^{b-1}$$

- If a primitive $3n/d$ -th root of unity ζ exists in \mathbb{Z}_q ,

$$R_q \cong \prod_{i=1}^{n/d} \mathbb{Z}_q[x] / \langle x^d - \zeta_i \rangle$$

where $\zeta_i \in \{\zeta^k \mid k \equiv \pm 1 \pmod{6}\}$.

- In NTRU+, small values $d \in \{3, 4\}$ are used.

Advantage of the Product Ring

- Original ring: $\mathbb{Z}_q[x]/\langle x^n - x^{n/2} + 1 \rangle$
 - Multiplication cost (naïve): $O(n^2)$
- Product ring: $\prod_{i=1}^{n/d} \mathbb{Z}_q[x]/\langle x^d - \zeta_i \rangle$
 - Multiplication cost (naïve): $O(nd)$
- Since $d \ll n$, $O(nd) \ll O(n^2)$.

How can we efficiently realize the ring isomorphism?

\Rightarrow Number Theoretic Transform (NTT)

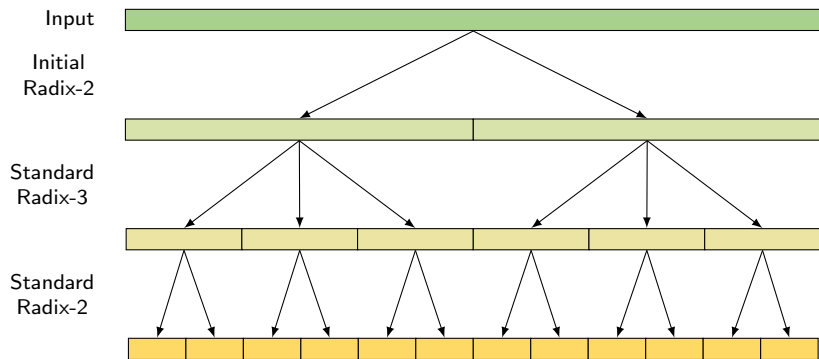
Mixed Radix NTT in NTRU+

- $R_q = \mathbb{Z}_q[x] / \langle x^n - x^{n/2} + 1 \rangle$, $n = 2^a 3^{b-1}$
- NTRU+ uses three types of NTT layers in the following order:
 - Initial Radix-2 NTT layer [5]
 - Standard Radix-3 NTT layers [3]
 - Standard Radix-2 NTT layers [1]

n	q	Initial Radix-2	Standard Radix-3	Standard Radix-2	d	ζ	$\ell = 3n/d$
768	3457	1	1	5	4	22	576
864	3457	1	2	4	3	9	864
1152	3457	1	2	4	4	9	864

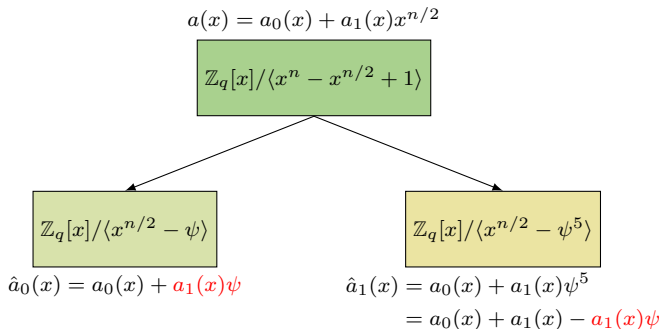
Table: NTT layer configurations

Example of Mixed Radix NTT



Initial Radix-2 NTT Layer

- Evaluation at two inputs (ψ, ψ^5)
 - ψ : a primitive sixth root of unity modulo q

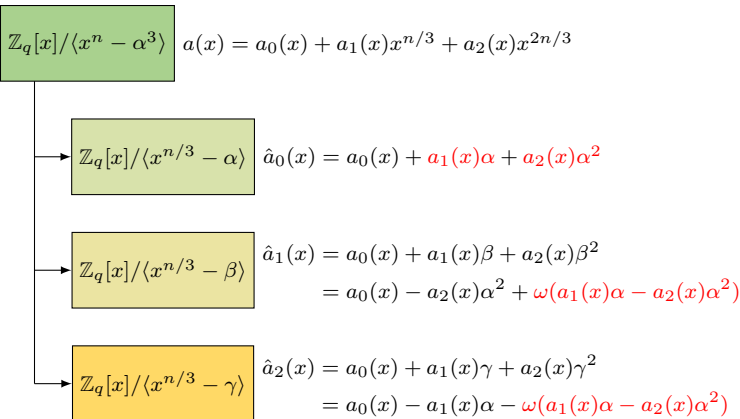


$$2a_0(x) = \hat{a}_0(x) + \hat{a}_1(x) - a_1(x)$$

$$a_1(x) = (\hat{a}_0(x) - \hat{a}_1(x))(\psi - \psi^5)^{-1}$$

Standard Radix-3 NTT Layer (1)

- Evaluation at three inputs: $(\alpha, \beta, \gamma) = (\alpha, \alpha\omega, \alpha\omega^2)$
 - ω : a primitive third root of unity modulo q



Standard Radix-3 NTT Layer (2)

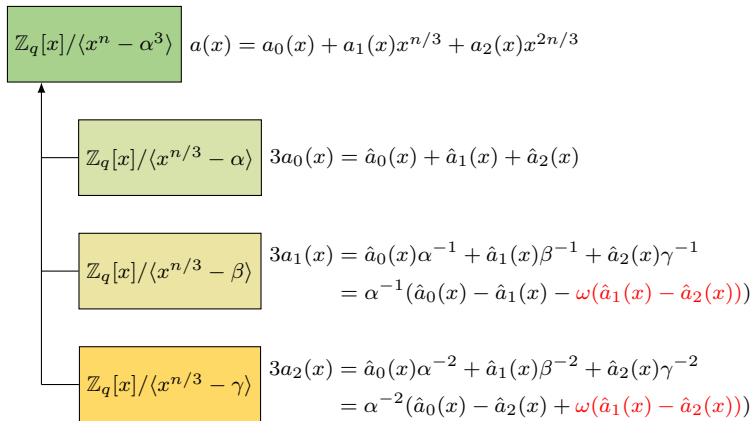
- NTT

$$\begin{pmatrix} \hat{a}_0(x) \\ \hat{a}_1(x) \\ \hat{a}_2(x) \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix}$$

- Inverse NTT

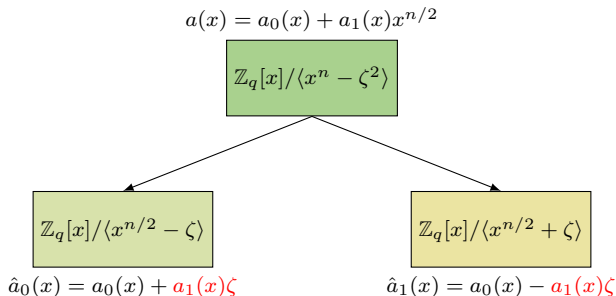
$$\begin{pmatrix} 1 & 1 & 1 \\ \alpha^{-1} & \beta^{-1} & \gamma^{-1} \\ \alpha^{-2} & \beta^{-2} & \gamma^{-2} \end{pmatrix} \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix} = 3 \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix}$$

Standard Radix-3 NTT Layer (3)



Standard Radix-2 NTT Layer

- Evaluation at two inputs $(\zeta, -\zeta)$



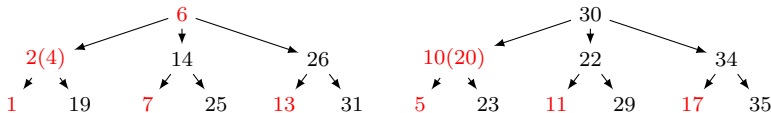
$$2a_0(x) = \hat{a}_0(x) + \hat{a}_1(x)$$

$$2a_1(x) = (\hat{a}_0(x) - \hat{a}_1(x))\zeta^{-1}$$

Example for $n = 24$, $d = 2$ ($3n/d = 36$)

- $\mathbb{Z}_q[x]/\langle x^{24} - x^{12} + 1 \rangle \approx \prod_{i=1}^{12} \mathbb{Z}_q[x]/\langle x^2 - \zeta_i \rangle$
 - ζ : primitive 36-th root of unity modulo q .
 - $\zeta^{18} \equiv -1 \pmod{q}$, $\psi \equiv \zeta^6 \pmod{q}$, $\omega \equiv \zeta^{12} \pmod{q}$

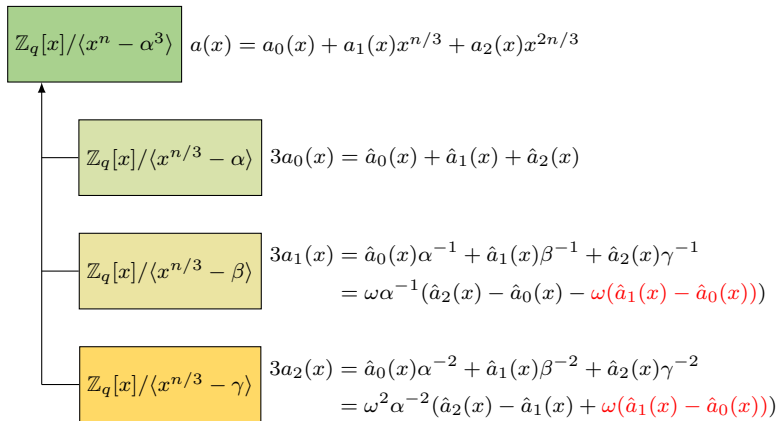
$$\begin{aligned}
 - \quad x^{24} - x^{12} + 1 &= (x^{12} - \zeta^6)(x^{12} - \zeta^{30}) \\
 &= (x^4 - \zeta^2)(x^4 - \zeta^{14})(x^4 - \zeta^{26})(x^4 - \zeta^{10})(x^4 - \zeta^{22})(x^4 - \zeta^{34}) \\
 &= (x^2 - \zeta)(x^2 - \zeta^{19})(x^2 - \zeta^7)(x^2 - \zeta^{25})(x^2 - \zeta^{13})(x^2 - \zeta^{31}) \\
 &\quad (x^2 - \zeta^5)(x^2 - \zeta^{23})(x^2 - \zeta^{11})(x^2 - \zeta^{29})(x^2 - \zeta^{17})(x^2 - \zeta^{35})
 \end{aligned}$$



$$\zeta^2 \zeta^{10} \equiv \zeta^{12} \equiv \omega \pmod{q} \quad \Rightarrow \quad \omega \zeta^{-2} \equiv \zeta^{10} \pmod{q}$$

$$\zeta^1 \zeta^{17} \equiv \zeta^{18} \equiv -1 \pmod{q} \quad \Rightarrow \quad \zeta^{-1} \equiv -\zeta^{17} \pmod{q}$$

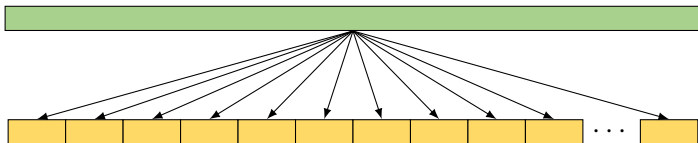
Standard Radix-3 NTT Layer (4)



Arithmetic in the NTT Domain

- Addition / Subtraction \Rightarrow unchanged
- Multiplication / Inversion \Rightarrow component-wise

$$\mathbb{Z}_q[x]/\langle x^n - x^{n/2} + 1 \rangle \cong \prod_{i=1}^{n/d} \mathbb{Z}_q[x]/\langle x^d - \zeta_i \rangle$$



Arithmetic in $\mathbb{Z}_q[x]/\langle x^d - \zeta \rangle$ ($d = 2$)

- Let $a(x) = a_0 + a_1x$, $b(x) = b_0 + b_1x \in \mathbb{Z}_q[x]/\langle x^2 - \zeta \rangle$

- Multiplication

- $c(x) = a(x)b(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + a_1b_1x^2$
 $= (a_0b_0 + a_1b_1\zeta) + (a_0b_1 + a_1b_0)x$

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} a_0 & a_1\zeta \\ a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

- Inversion

- If $b(x) = a(x)^{-1}$, then

$$\begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_0 & a_1\zeta \\ a_1 & a_0 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{a_0^2 - a_1^2\zeta} \begin{bmatrix} a_0 \\ -a_1 \end{bmatrix}$$

Arithmetic in $\mathbb{Z}_q[x]/\langle x^d - \zeta \rangle$ ($d = 3$)

- Multiplication

- $c(x) = a(x)b(x)$

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a_0 & a_2\zeta & a_1\zeta \\ a_1 & a_0 & a_2\zeta \\ a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix}$$

- Inversion

- If $b(x) = a(x)^{-1}$, then

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_0 & a_2\zeta & a_1\zeta \\ a_1 & a_0 & a_2\zeta \\ a_2 & a_1 & a_0 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = d^{-1} \begin{bmatrix} a'_0 \\ a'_1 \\ a'_2 \end{bmatrix}$$

where

$$\begin{aligned} a'_0 &= a_0^2 - \zeta a_1 a_2, & a'_1 &= \zeta a_2^2 - a_0 a_1, & a'_2 &= a_1^2 - a_0 a_2, \\ d &= a_0 a'_0 + \zeta(a_1 a'_2 + a_2 a'_1) = a_0^3 - 3\zeta a_0 a_1 a_2 + \zeta a_1^3 + \zeta^2 a_2^3. \end{aligned}$$

Arithmetic in $\mathbb{Z}_q[x]/\langle x^d - \zeta \rangle$ ($d = 4$) (1)

- Multiplication

- $c(x) = a(x)b(x)$

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3\zeta & a_2\zeta & a_1\zeta \\ a_1 & a_0 & a_3\zeta & a_2\zeta \\ a_2 & a_1 & a_0 & a_3\zeta \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

- Inversion

- If $b(x) = a(x)^{-1}$, then

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3\zeta & a_2\zeta & a_1\zeta \\ a_1 & a_0 & a_3\zeta & a_2\zeta \\ a_2 & a_1 & a_0 & a_3\zeta \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Direct inversion ignores the ring structure

Arithmetic in $\mathbb{Z}_q[x]/\langle x^d - \zeta \rangle$ ($d = 4$) (2)

- Inversion in $\mathbb{Z}_q[x]/\langle x^4 - \zeta \rangle$ can be reduced to inversion in $\mathbb{Z}_q[z]/\langle z^2 - \zeta \rangle$ with $z = x^2$ [6].
- Let $z = x^2$ and write

$$a(x) = a_0 + a_1x + a_2x^2 + a_3x^3 = \tilde{a}_0(z) + \tilde{a}_1(z)x$$

where $\tilde{a}_0(z) = a_0 + a_2z$ and $\tilde{a}_1(z) = a_1 + a_3z$.

- Then, for $b(x) = \tilde{b}_0(z) + \tilde{b}_1(z)x$ with $b(x) = a(x)^{-1}$,

$$\begin{bmatrix} \tilde{b}_0(z) \\ \tilde{b}_1(z) \end{bmatrix} = \begin{bmatrix} \tilde{a}_0(z) & \tilde{a}_1(z)z \\ \tilde{a}_1(z) & \tilde{a}_0(z) \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\tilde{a}_0^2(z) - \tilde{a}_1^2(z)z} \begin{bmatrix} \tilde{a}_0(z) \\ -\tilde{a}_1(z) \end{bmatrix}.$$

Inversion in \mathbb{Z}_q

- In all cases, we require inversion in \mathbb{Z}_q
- For constant-time execution, we use exponentiation
- By Fermat's little theorem:

$$\begin{aligned}\text{For } a \in \mathbb{Z}_q^*, \quad a^{q-1} &\equiv 1 \pmod{q} \\ \Rightarrow \quad a \cdot a^{q-2} &\equiv 1 \pmod{q}\end{aligned}$$

- Hence, exponentiation by $q - 2$ yields

$$a^{q-2} \equiv \begin{cases} a^{-1} & (a \in \mathbb{Z}_q^*), \\ 0 & (a = 0) \end{cases} \pmod{q}$$

Inversion in \mathbb{Z}_{3457}

- Square-and-Multiply for $q - 2 = 3455 = (110101111111)_2$
 - Total cost: 11 squarings + 5 multiplications

$$t_1 = a^2 \quad // \ 10$$

$$t_2 = t_1^2 = a^4 \quad // \ 100$$

$$t_2 = t_2^2 = a^8 \quad // \ 1000$$

$$t_3 = t_2^2 = a^{16} \quad // \ 10000$$

$$t_1 = t_1 \cdot t_2 = a^{10} // \ 1010$$

$$t_2 = t_1 \cdot t_3 = a^{26} // \ 11010$$

$$t_2 = t_2^2 = a^{52} \quad // \ 110100$$

$$t_2 = t_2 \cdot a = a^{53} // \ 110101$$

$$t_1 = t_1 \cdot t_2 = a^{63} \quad // \ 111111$$

$$t_2 = t_2^2 = a^{106} \quad // \ 1101010$$

$$t_2 = t_2^2 = a^{212} \quad // \ 11010100$$

$$t_2 = t_2^2 = a^{424} \quad // \ 110101000$$

$$t_2 = t_2^2 = a^{848} \quad // \ 1101010000$$

$$t_2 = t_2^2 = a^{1696} \quad // \ 11010100000$$

$$t_2 = t_2^2 = a^{3392} \quad // \ 110101000000$$

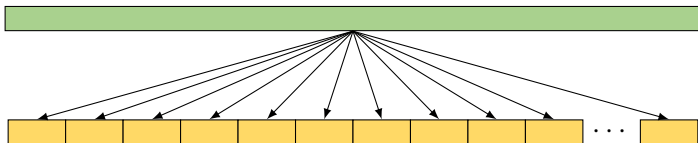
$$t_2 = t_2 \cdot t_1 = a^{3455} // \ 110101111111$$

Batch Inversion in NTT domain

- Batch inversion

- n/d inversions \Rightarrow 1 inversion + $3(n/d - 1)$ multiplications in \mathbb{Z}_q

$$\mathbb{Z}_q[x]/\langle x^n - x^{n/2} + 1 \rangle \cong \prod_{i=1}^{n/d} \mathbb{Z}_q[x]/\langle x^d - \zeta_i \rangle$$



Batch Inversion (Montgomery's Trick)

- For two elements:

$$(a_0, a_1) \Rightarrow (a_0^{-1}, a_1^{-1}) = \left(\frac{a_1}{a_0 a_1}, \frac{a_0}{a_0 a_1} \right)$$

Only one inversion: $(a_0 a_1)^{-1}$

- For three elements:

$$(a_0, a_1, a_2) \Rightarrow (a_0^{-1}, a_1^{-1}, a_2^{-1}) = \left(\frac{a_1 a_2}{a_0 a_1 a_2}, \frac{a_0 a_2}{a_0 a_1 a_2}, \frac{a_0 a_1}{a_0 a_1 a_2} \right)$$

Only one inversion: $(a_0 a_1 a_2)^{-1}$

Batch Modular Inversion (Montgomery's Trick)

Algorithm 1: BatchInv

Require: Array $a = (a_0, \dots, a_{k-1}) \in \mathbb{Z}_q^k$

Ensure: If $a_i \neq 0$ for all i , then $b_i = a_i^{-1}$; otherwise $b = (0, \dots, 0)$.

```
1:  $t_0 \leftarrow a_0$ 
2: for  $i = 1$  to  $k - 1$  do
3:    $t_i \leftarrow t_{i-1} \cdot a_i$ 
4:  $inv \leftarrow t_{k-1}^{-1}$ 
5: for  $i = k - 1$  downto  $1$  do
6:    $b_i \leftarrow t_{i-1} \cdot inv$ 
7:    $inv \leftarrow inv \cdot a_i$ 
8:  $b_0 \leftarrow inv$ 
9: return  $(b_0, \dots, b_{k-1})$ 
```

Resources

NTRU+ Official Resources

- Official homepage
 - <https://www.ntruplus.org/>
- GitHub repository for source code:
 - <https://github.com/ntruplus/ntruplus>
 - Reference implementation: C code focused on clarity and correctness
 - Optimized implementation: high-performance C code
 - Additional implementations: Intel AVX2 and ARMv8-A NEON
- Resources for NTT
 - <https://data.ntruplus.org/ntt.pdf>
 - https://github.com/ntruplus/ntt_for_ntruplus

Thank You for Your Attention!

Any Questions?

References



Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé.
CRYSTALS - Kyber: A CCA-secure module-lattice-based KEM.
In *2018 IEEE European Symposium on Security and Privacy*, pages 353–367. IEEE Computer Society Press, April 2018.



Julien Duman, Kathrin Hövelmanns, Eike Kiltz, Vadim Lyubashevsky, Gregor Seiler, and Dominique Unruh.
A thorough treatment of highly-efficient NTRU instantiations.
In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *PKC 2023, Part I*, volume 13940 of *LNCS*, pages 65–94. Springer, Cham, May 2023.



Chenar Abdulla Hassan and Oğuz Yayla.
Radix-3 NTT-based polynomial multiplication for lattice-based cryptography.
Cryptography ePrint Archive, Report 2022/726, 2022.



Jonghyun Kim and Jong Hwan Park.
NTRU+: Compact Construction of NTRU Using Simple Encoding Method.
IEEE Transactions on Information Forensics and Security, 18:4760–4774, 2023.



Vadim Lyubashevsky and Gregor Seiler.
NTTRU: Truly fast NTRU using NTT.
IACR TCHES, 2019(3):180–201, 2019.



Jiang Zhang, Dengguo Feng, and Di Yan.
NEV: Faster and smaller NTRU encryption using vector decoding.
In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part VII*, volume 14444 of *LNCS*, pages 157–189. Springer, Singapore, December 2023.

Appendix

Initial Radix-2 NTT Layer

- $R_q = \mathbb{Z}_q[x]/\langle x^n - x^{n/2} + 1 \rangle$
 - ψ : primitive 6-th root of unity modulo q
 - $\psi^i \not\equiv 1 \pmod{q}$ for $i \in [1, 5]$
 - $\psi^6 \equiv 1 \pmod{q}$
 - **Fact 1:** $\psi^2 - \psi + 1 \equiv 0 \pmod{q}$
 - $\psi^6 - 1 \equiv (\psi^3 - 1)(\psi + 1)(\psi^2 - \psi + 1) \equiv 0 \pmod{q}$
 - By the definition of ψ , $\psi^2 - \psi + 1 \equiv 0 \pmod{q}$
 - **Fact 1-1:** $\psi^3 + 1 \equiv (\psi + 1)(\psi^2 - \psi + 1) \equiv 0 \pmod{q}$
 - **Fact 2:** $x^2 - x + 1 = (x - \psi)(x - \psi^5)$
 - $(x - \psi)(x - \psi^5) \equiv x^2 - (\psi + \psi^5) + \psi^6 \pmod{q}$
 - **Fact 2-1:** $\psi + \psi^5 \equiv \psi - \psi^2 \equiv 1 \pmod{q}$
 - $\psi^6 \equiv 1 \pmod{q}$
 - $x^n - x^{n/2} + 1 = (x^{n/2} - \psi)(x^{n/2} - \psi^5)$ (\because **Fact 2**)

Standard Radix-3 NTT Layer

- $R_q = \mathbb{Z}_q[x] / \langle x^3 - \zeta^3 \rangle$
 - ω : primitive 3-th root of unity modulo q
 - $\omega^i \not\equiv 1 \pmod{q}$ for $i \in [1, 2]$
 - $\omega^3 \equiv 1 \pmod{q}$
 - **Fact 1:** $\omega^2 + \omega + 1 \equiv 0 \pmod{q}$
 - $\omega^3 - 1 \equiv (\omega - 1)(\omega^2 + \omega + 1) \equiv 0 \pmod{q}$
 - By the definition of ω , $\omega^2 + \omega + 1 \equiv 0 \pmod{q}$
 - **Fact 2:** $x^3 - \zeta^3 = (x - \alpha)(x - \beta)(x - \gamma)$
 - $\alpha = \zeta, \beta = \zeta\omega, \gamma = \zeta\omega^2$
 - $(x - \alpha)(x - \beta)(x - \gamma) = x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha\beta + \beta\gamma + \gamma\alpha)x - \alpha\beta\gamma$
 - $\alpha + \beta + \gamma \equiv \zeta(1 + \omega + \omega^2) \equiv 0 \pmod{q}$ (\because **Fact 1**)
 - $\alpha\beta + \beta\gamma + \gamma\alpha \equiv \zeta(\omega + \omega^3 + \omega^2)$
 $\equiv \zeta(1 + \omega + \omega^2) \equiv 0 \pmod{q}$ (\because **Fact 1**)
 - $\alpha\beta\gamma \equiv \zeta^3\omega^3 \equiv \zeta^3 \pmod{q}$

Standard Radix-3 NTT layer

- NTT

$$\begin{pmatrix} \hat{a}_0(x) \\ \hat{a}_1(x) \\ \hat{a}_2(x) \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix}$$

- Inverse NTT

$$\begin{pmatrix} 1 & 1 & 1 \\ \alpha^{-1} & \beta^{-1} & \gamma^{-1} \\ \alpha^{-2} & \beta^{-2} & \gamma^{-2} \end{pmatrix} \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix} = 3 \begin{pmatrix} a_0(x) \\ a_1(x) \\ a_2(x) \end{pmatrix}$$

- $\alpha^2 + \beta^2 + \gamma^2 \equiv (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) \equiv 0 \pmod{q}$
- $\alpha^{-1} + \beta^{-1} + \gamma^{-1} \equiv (\alpha\beta\gamma)^{-1}(\alpha\beta + \beta\gamma + \gamma\alpha) \equiv 0 \pmod{q}$
- $\alpha^{-2} + \beta^{-2} + \gamma^{-2}$
 $\equiv (\alpha^{-1} + \beta^{-1} + \gamma^{-1})^2 - 2(\alpha^{-1}\beta^{-1} + \beta^{-1}\gamma^{-1} + \gamma^{-1}\alpha^{-1})$
 $\equiv (\alpha^{-1} + \beta^{-1} + \gamma^{-1})^2 - 2\alpha^{-1}\beta^{-1}\gamma^{-1}(\alpha + \beta + \gamma) \equiv 0 \pmod{q}$