

NTRU+

**Compact Construction of NTRU
Using Simple Encoding Method**

2023.02.22.

상명대학교

박종환

Contents

1. 배경지식
2. NTRU
3. Correctness
4. ACWC
5. 제안기법
6. Parameters
7. NTRU+ PKE



❖ Ring $R_q = \mathbb{Z}_q[x]/f(x)$

◆ Modulus q , polynomial $f(x)$ of degree n

❖ Ring $R_q = \mathbb{Z}_q[x]/f(x) = \{a_0 + a_1x + \dots + a_nx^{n-1} \mid a_i \in \mathbb{Z}_q\}$

◆ Representation:

$$\mathbf{a}(x) = a_0 + a_1x + \dots + a_nx^{n-1} \leftrightarrow (a_0, a_1, \dots, a_{n-1}) \in (\mathbb{Z}_q)^n$$

$$\mathbf{b}(x) = b_0 + b_1x + \dots + b_nx^{n-1} \leftrightarrow (b_0, b_1, \dots, b_{n-1}) \in (\mathbb{Z}_q)^n$$

◆ Addition/subtraction:

$$\begin{aligned} (a_0, a_1, \dots, a_{n-1}) \pm (b_0, b_1, \dots, b_{n-1}) \\ = (a_0 \pm b_0, a_1 \pm b_1, \dots, a_{n-1} \pm b_{n-1}) \end{aligned}$$

◆ Multiplication:

$$(a_0, a_1, \dots, a_{n-1}) \times (b_0, b_1, \dots, b_{n-1}) = (c_0, c_1, \dots, c_{n-1})$$

◆ Division:

$$(a_0, a_1, \dots, a_{n-1}) \times (b_0, b_1, \dots, b_{n-1}) = 1 \text{ in } R_q$$

Using NTT

❖ Ring $R_q = \mathbb{Z}_q[x]/f(x)$

◆ $f(x) = x^n + 1$, where $n = 2^k$ - **KYBER, FALCON, Dilithium**

◆ $f(x) = x^n - 1$, where n is prime - **NTRU**

❖ $R_q = \mathbb{Z}_q[x]/\langle x^n + 1 \rangle$ ($n = 2^k$)

+ Easy to implement NTT

– Sparse $n = 256, 512, 1024, \dots$

Security($n = 512$) < 128

Security($n = 1024$) \gg 128

❖ $R_q = \mathbb{Z}_q[x]/\langle x^n - 1 \rangle$ ($n = \text{prime}$)

– Hard to implement NTT

+ Dense $n = 521, 523, 542, 547, 557, 563, 569, \dots$

- ❖ Ring $R_q = \mathbb{Z}_q[x]/f(x)$
 - ◆ $f(x) = x^n + 1$, where $n = 2^k$ - **KYBER, FALCON, Dilithium**
 - ◆ $f(x) = x^n - 1$, where n is prime - **NTRU**
 - ◆ $f(x) = x^n - x^{\frac{n}{2}} + 1$, where $n = 2^i 3^j$ - **NTRU+**

- ❖ $R_q = \mathbb{Z}_q[x]/\langle x^n - x^{n/2} + 1 \rangle$ ($n = 2^i 3^j$)
 - + Easy to implement NTT [LS19]
 - + Moderate $n = \mathbf{512}, 576, 648, 768, 864, 972, \mathbf{1024}, \dots$

❖ $\text{CBD}_1(u)$

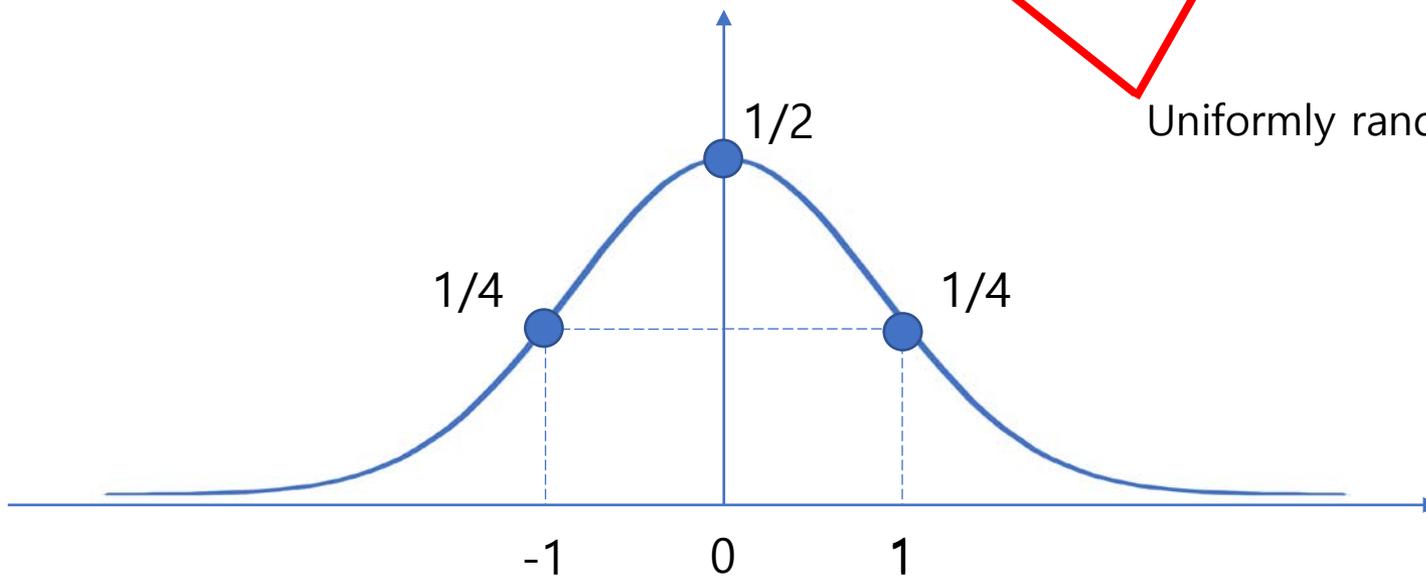
◆ $u = (u_0, u_1) \leftarrow_u \{0,1\}^{2n}$

◆ **return** $y = u_0 - u_1$ (component-wise)

0	-	0	=	0
1		1		0
0		1		-1
1		0		1

$u_0 - u_1 = y$

Uniformly random bits



❖ PKE

- ◆ KeyGen \rightarrow (pk, sk)
- ◆ Enc(pk, m ; r) = C
- ◆ Dec(sk, C) = m

❖ Correctness: Dec(sk, Enc(pk, m ; r)) = m

- ◆ Average-case correctness error

$$\Pr_{m \leftarrow \psi_{\mathcal{M}}, r \leftarrow \psi_{\mathcal{R}}} [Dec(sk, Enc(pk, m; r)) \neq m] \leq \delta$$

- ◆ Worst-case correctness error

$$\Pr_{m \in \psi_{\mathcal{M}}, r \in \psi_{\mathcal{R}}} [Dec(sk, Enc(pk, m; r)) \neq m] \leq \delta$$

- ◆ Perfect correctness error

$$\Pr_{\forall m \in \psi_{\mathcal{M}}, \forall r \in \psi_{\mathcal{R}}} [Dec(sk, Enc(pk, m; r)) \neq m] = 0$$

❖ In a ring $R_q = \mathbb{Z}_q[x] / (x^n - 1)$

◆ (n, q) chosen and small prime $p = 3$

❖ Ring $R_q = \mathbb{Z}_q[x] / f(x) = \{a_0 + a_1x + \dots + a_n x^{n-1} \mid a_i \in \mathbb{Z}_q\}$

▪ Representation

$$\mathbf{a}(x) = a_0 + a_1x + \dots + a_n x^{n-1} \leftrightarrow (a_0, a_1, \dots, a_{n-1})$$

$\in \mathbb{Z}_q \times \mathbb{Z}_q \times \dots \times \mathbb{Z}_q$

❖ Ring $R_p = \mathbb{Z}_p[x] / f(x) = \{a_0 + a_1x + \dots + a_n x^{n-1} \mid a_i \in \mathbb{Z}_p\}$

▪ Representation

$$\mathbf{a}(x) = a_0 + a_1x + \dots + a_n x^{n-1} \leftrightarrow (a_0, a_1, \dots, a_{n-1})$$

$\in \mathbb{Z}_p \times \mathbb{Z}_p \times \dots \times \mathbb{Z}_p$

▪ $p \ll q$

❖ Example of NTRU ring

- $f(x) = x^{509} - 1$ ($n = 509$), $q = 2^{11}$, $p = 3$
- Coefficients of (f, g) chosen in $[-1, 1]$ in R_p
 - $f = 1 - x + x^3 - x^7 + \dots + x^{504} - x^{508}$
 - $g = 1 + x^2 - x^5 + x^{10} - \dots - x^{506} - x^{507}$
- f_q^{-1} (in R_q) = $-1011 + 488x + 964x^2 - 815x^3 - \dots + 735x^{507} - 633x^{508}$
- f_p^{-1} (in R_p) = $-1 + x + x^2 - x^3 - \dots + x^{506} - x^{508}$
- $h = g \cdot f_q^{-1}$ (in R_q) = $-976 - 288x + 519x^2 + 852x^3 + \dots - 1021x^{507} + 491x^{508}$
- Coefficients of (r, m) chosen in $[-1, 1]$ in R_p
 - $r = -1 + x - x^2 - x^5 + \dots + x^{506} + x^{508}$
 - $m = 1 + x + x^4 - x^5 - \dots + x^{506} - x^{507}$
- $c = ph \cdot r + m$ (in R_q) = $277 + 993x + \dots + 1001x^{507} - 388x^{508}$

$[-1, 1]$ in R_p

$[-1024, 1024]$ in R_q

$[-1, 1]$ in R_p

❖ $R_q = \mathbb{Z}_q[x] / \langle x^n - 1 \rangle$, $p = 3$ scalar multiplication

◆ **Public key** : $h = p(g \cdot f_q^{-1}) \in R_q$ **Secret key** : f, f_p^{-1}

◆ **Ciphertext** : $c = r \cdot h + m \in R_q$

$m, r \leftarrow \mathcal{T}_{fixed-weight}$

$f, g \leftarrow \mathcal{T}_{uniform}$

PK : $h = p \cdot g \cdot f_q^{-1}$ SK : f, f_p^{-1}

The diagram illustrates the public key generation. On the left, a dark blue vertical bar labeled 'h' is shown. To its right is an equals sign. Further right is a light grey vertical bar labeled 'p', followed by a dot, a light orange vertical bar labeled 'g', followed by another dot, and a blue vertical bar labeled 'f_q^{-1}'. A large blue bracket on the right side of these three bars indicates the result is in the ring R_q. To the right of this equation, the secret key is shown as two blue vertical bars labeled 'f' and 'f_p^{-1}'.

CT : $c = r \cdot h + m$

The diagram illustrates the ciphertext generation. On the left, a black vertical bar labeled 'c' is shown. To its right is an equals sign. Further right is a light green vertical bar labeled 'r', followed by a dot, a dark blue vertical bar labeled 'h', followed by a plus sign, and a yellow vertical bar labeled 'm'. A large blue bracket on the right side of these three bars indicates the result is in the ring R_q.

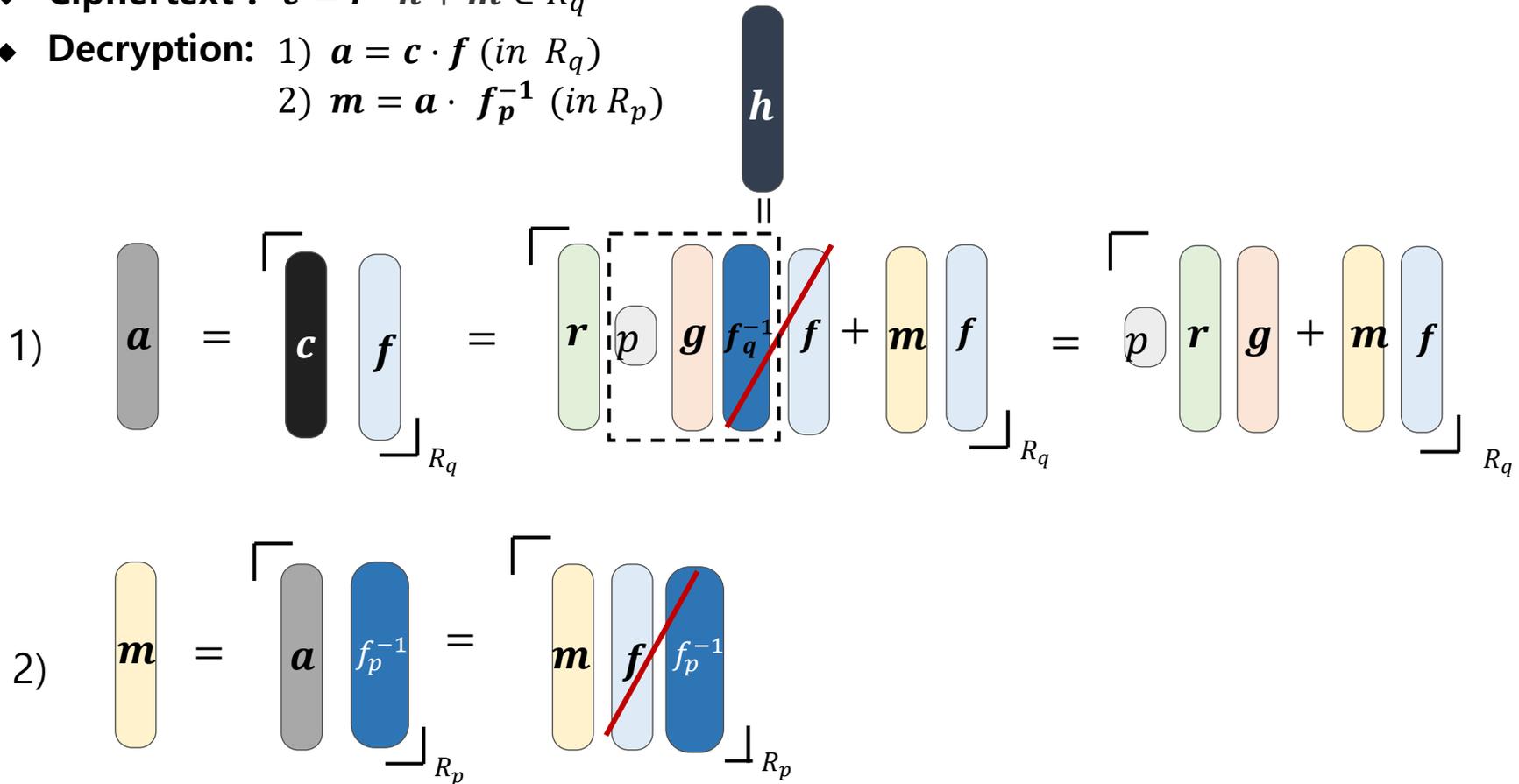
- $\mathcal{T}_{fixed-weight}$: fixed-weight ternary distribution (e.g., $n = 743$, $h = 494$)
- $\mathcal{T}_{uniform}$: uniform distribution among $\{-1, 0, 1\}$

$$\diamond R_q = \mathbb{Z}_q[x] / \langle x^n - 1 \rangle, \quad p = 3$$

$$\diamond \text{Public key : } h = p(g \cdot f_q^{-1}) \in R_q \quad \text{Secret key : } f, f_p^{-1}$$

$$\diamond \text{Ciphertext : } c = r \cdot h + m \in R_q$$

$$\diamond \text{Decryption: } \begin{array}{l} 1) a = c \cdot f \text{ (in } R_q) \\ 2) m = a \cdot f_p^{-1} \text{ (in } R_p) \end{array}$$



$$\diamond R_q = \mathbb{Z}_q[x] / \langle x^n - 1 \rangle, \quad p = 3$$

$$\diamond \text{Public key : } h = p(g \cdot f_q^{-1}) \in R_q \quad \text{Secret key : } f, f_p^{-1}$$

$$\diamond \text{Ciphertext : } c = r \cdot h + m \in R_q$$

$$\diamond \text{Decryption: } \begin{array}{l} 1) a = c \cdot f \text{ (in } R_q) \\ 2) m = a \cdot f_p^{-1} \text{ (in } R_p) \end{array}$$

- Decryption works only when all coefficients of $a = p(r \cdot g) + m \cdot f \in [-q/2, q/2]$

$$a = p \cdot r \cdot g + m \cdot f$$

This part = 0 (mod p) if $|p(r \cdot g) + m \cdot f|_\infty < q/2$

- ◆ Distributions D_f, D_g, D_r, D_m are important for correctness of NTRU

$$\diamond R_q = \mathbb{Z}_q[x] / \langle x^n - 1 \rangle, \quad p = 3$$

◆ **Public key :** $h = p(g \cdot f^{-1}) \in R_q$ **Secret key :** f

▪ $f = 3f' + 1$, where f' chosen in R_p

$$f = 3f' + 1$$

◆ **Ciphertext :** $c = r \cdot h + m \in R_q$

$$\text{PK : } h = p \cdot g \cdot f^{-1} \quad \text{SK : } f$$

$$\text{CT : } c = r \cdot h + m$$

▪ Coefficients of f' are chosen from $D_{f'}$

$$\diamond R_q = \mathbb{Z}_q[x] / \langle x^n - 1 \rangle, \quad p = 3$$

◆ **Public key :** $h = p(g \cdot f^{-1}) \in R_q$ **Secret key :** f

▪ $f = 3f' + 1$, where f' chosen in R_p

◆ **Ciphertext :** $c = r \cdot h + m \in R_q$

◆ **Decryption:** $m = c \cdot f$ (in R_q) (mod p)

$$f = 3f' + 1$$

$$\begin{aligned}
 m &= \left[\begin{array}{c} c \\ f \end{array} \right]_{R_q} = \left[\begin{array}{c} r \\ p \end{array} \right] \left[\begin{array}{c} g \\ f^{-1} \\ f \end{array} \right] + \left[\begin{array}{c} m \\ f \end{array} \right]_{R_q} = \left[\begin{array}{c} p \\ r \\ g \end{array} \right] + \left[\begin{array}{c} m \\ f \end{array} \right]_{R_q} \\
 &= \left[\begin{array}{c} p \\ r \\ g \end{array} \right] + \left[\begin{array}{c} p \\ m \\ f' \end{array} \right] + \left[\begin{array}{c} m \end{array} \right]_{R_q}
 \end{aligned}$$

$$\diamond R_q = \mathbb{Z}_q[x] / \langle x^n - 1 \rangle, \quad p = 3$$

◆ **Public key :** $h = p(g \cdot f^{-1}) \in R_q$ **Secret key :** f

▪ $f = 3f' + 1$, where f' chosen in R_p

$$f = 3f' + 1$$

◆ **Ciphertext :** $c = r \cdot h + m \in R_q$

◆ **Decryption:** $m = c \cdot f$ (in R_q) (mod p)

▪ Decryption works only when all coefficients of $p(r \cdot g + m \cdot f') + m \in [-q/2, q/2]$

$$m = p \cdot r \cdot g + p \cdot m \cdot f' + m$$

This part = 0 (mod p) if $|p(r \cdot g + m \cdot f') + m|_\infty < q/2$

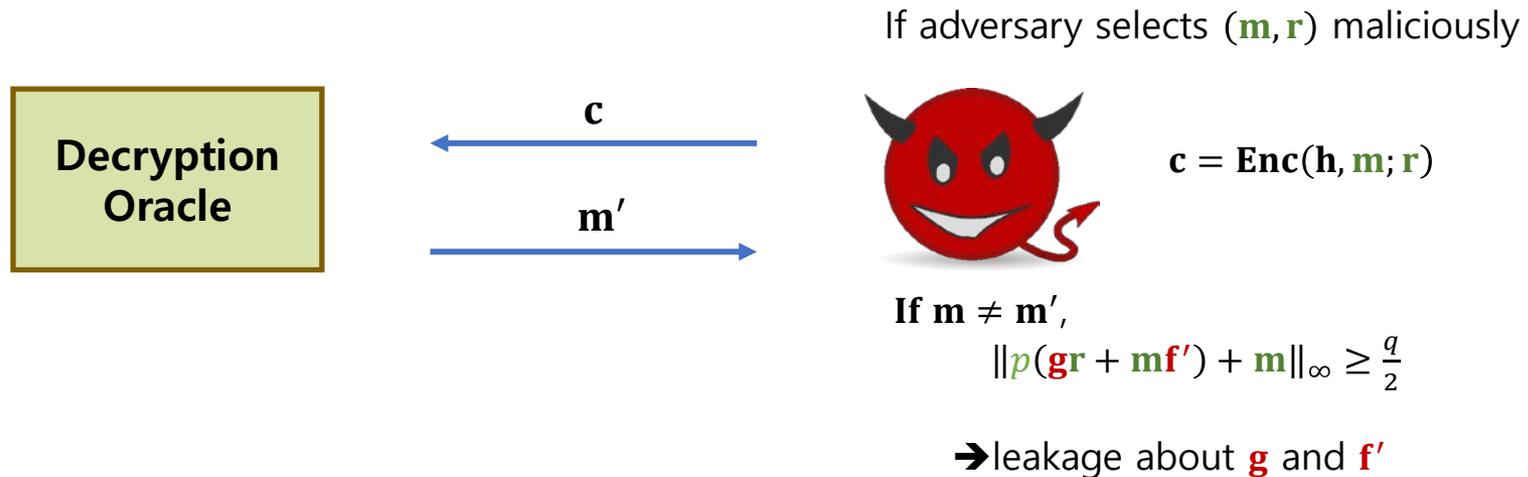
◆ **Distributions $D_{f'}, D_g, D_r, D_m$ are important for correctness of NTRU**

❖ Correctness error of NTRU

- ◆ $|p(r \cdot g) + m \cdot f|_\infty < q/2$
- ◆ $|p(r \cdot g + m \cdot f') + m|_\infty < q/2$

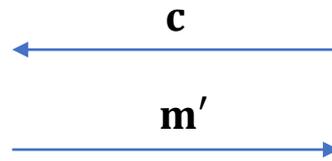
❖ In achieving worst-case correctness error (in IND-CCA)

- ◆ Adversary can have control over r and m , but . . .



❖ In ElGamal-type PKE/KEM (like Kyber)

Decryption
Oracle



If adversary selects (\mathbf{m}, \mathbf{r}) maliciously



$$c = \text{Enc}(\mathbf{h}, \mathbf{m}; \mathbf{r})$$

If $\mathbf{m} \neq \mathbf{m}'$,

$$\| \mathbf{r} \cdot \mathbf{e} + \mathbf{e}_2 - \mathbf{e}_1 \cdot \mathbf{s} \|_{\infty} \geq \frac{q}{4}$$

→ \mathbf{m} is not relevant of correctness

◆ Using Fujisaki-Okamoto (FO) transform [HHK17]

- $H(m) = r$
- $c = \text{Enc}(pk, m; r)$

Fortunately,

It is hard to control $r = (r, e_1, e_2)$ when FO transform is applied

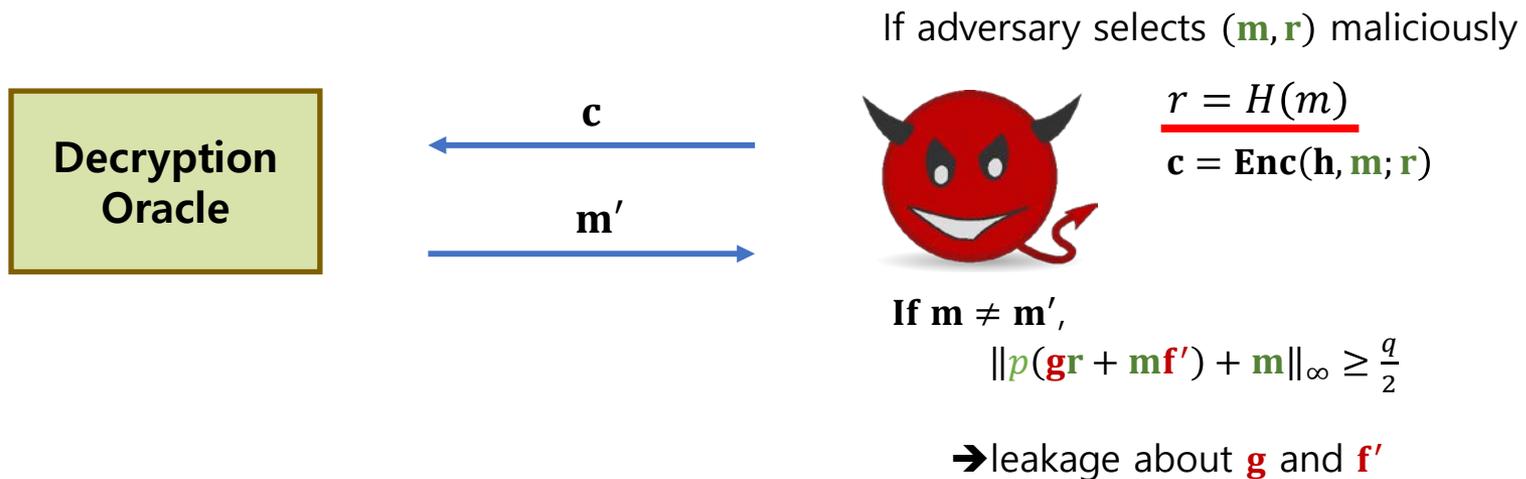
◆ Average-case correctness error \approx worst-case correctness error

❖ Correctness error of NTRU

- ◆ $|p(r \cdot \mathbf{g}) + \mathbf{m} \cdot \mathbf{f}|_\infty < q/2$
- ◆ $|p(r \cdot \mathbf{g} + \mathbf{m} \cdot \mathbf{f}') + \mathbf{m}|_\infty < q/2$

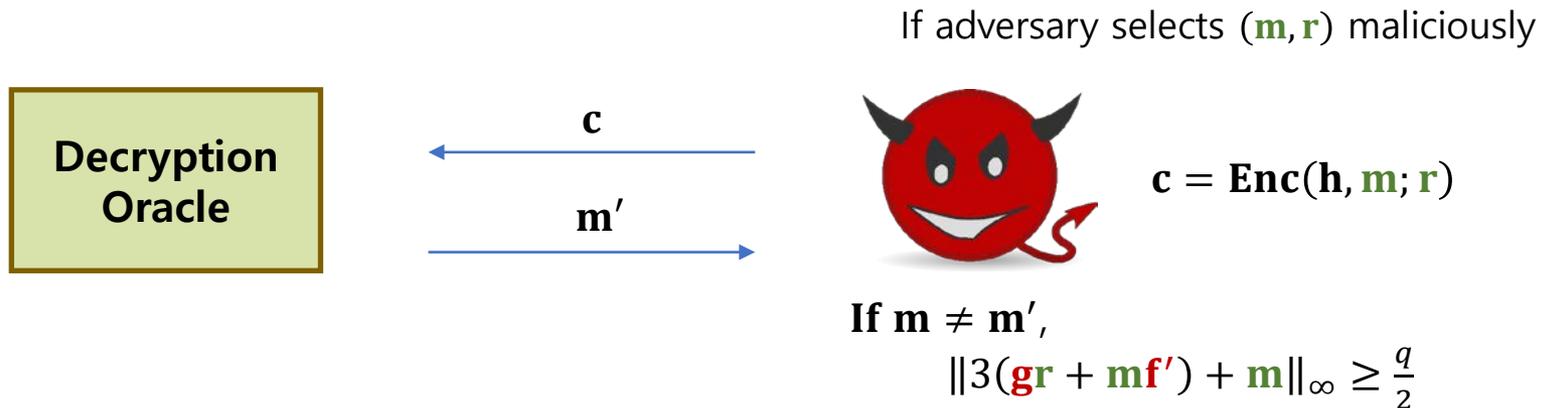
❖ When using FO-transform

- ◆ Hard to control r , but still adversary can control m



- ◆ Not easy to achieve worst-case correctness error of NTRU

❖ How to achieve worst-case correctness error

◆ **Solution 1 – perfect correctness error**

- All (m, r) tuples do not make NTRU decryption fail
- Require modulus q to be relatively large
- Adopted by **Finalist NTRU**

◆ **Solution 2 - worst-case correctness error**

- An encoding method that forces m (as well as r) to be sampled honestly
- Introduced in NTRU-B [DHK+21], but incomplete
- Improved by NTRU+ [KP22]

[DHK+21] Duman et al. "A Thorough Treatment of Highly-Efficient NTRU Instantiations", <https://eprint.iacr.org/2021/1352.pdf>

[KP22] Kim et al. "NTRU+: Compact Construction of NTRU Using Simple Encoding Method", <https://eprint.iacr.org/2022/1664.pdf>

❖ Generalized One-time Pad (GOTP)

- ◆ U_3 distribution: uniformly random over $\{-1, 0, 1\}$
- ◆ $u \leftarrow U_3^n$

❖ GOTP for NTRU-B [DHK+21]

◆ $\text{GOTP}(x, u) = y$

▪ $y = x + u \pmod{\pm 3}$

$$\begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \pmod{\pm 3} = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}$$

$x \qquad u \qquad y$

◆ $\text{Inv}(y, u) = x \in \{-1, 0, 1\}^n$

▪ $x = y - u \pmod{\pm 3}$

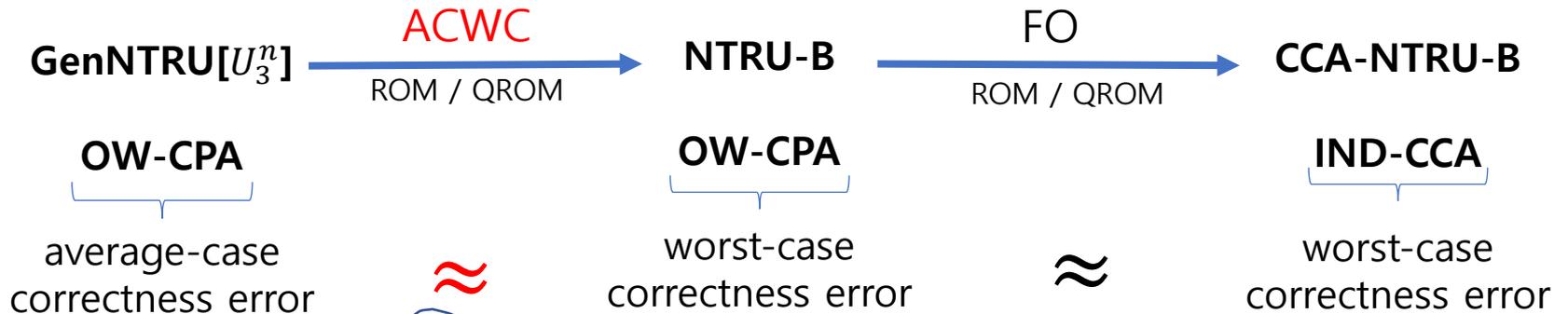
$$\begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} - \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \pmod{\pm 3}$$

$x \qquad y \qquad u$

❖ ACWC transform [DHK+21]

◆ GenNTRU[U_3^n]

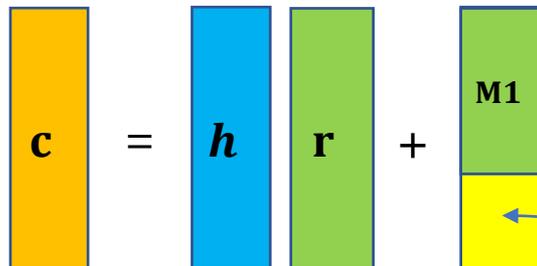
- (f, g, M, r) are sampled uniformly at random over $\{-1, 0, 1\}$



$$- (r, M_1) \leftarrow U_3^n$$

$$- M \leftarrow M_1 || \text{GOTP}(m, G(M_1))$$

$$- \text{Enc}(pk, M; r) = c$$



$$\text{Message } m \leftarrow U_3^n$$

$$\text{GOTP}(m, G(M_1)) \in U_3^{n-\gamma}$$

Scheme	NTRU [CDH+20]	NTRU-B [DHK+21]	NTRU+[KP22]
NTT-friendly	No	Yes	Yes
Correctness error	Perfect	Worst-case	Worst-case
(m, r) -encoding	No	Yes	Yes
Message set	$(\mathbf{m}, \mathbf{r}) \leftarrow \{-1, 0, 1\}^n$	$m \leftarrow \{-1, 0, 1\}^\lambda$	$m \leftarrow \{0, 1\}^n$
Message distribution	Uniform/Fixed-weight	Uniform	Arbitrary
CCA transform	DPKE + SXY variant	ACWC + FO [⊥]	ACWC ₂ + $\overline{\text{FO}}^\perp$
Assumptions	NTRU, RLWE	NTRU, RLWE	NTRU, RLWE
Tight reduction	Yes	No	Yes

[CDH+20] C. Chen et al., NTRU. Technical report, National Institute of Standards and Technology, 2020. available at <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions>

[DHK+21] Duman et al. "A Thorough Treatment of Highly-Efficient NTRU Instantiations", <https://eprint.iacr.org/2021/1352.pdf>

[KP22] Kim et al. "NTRU+: Compact Construction of NTRU Using Simple Encoding Method", <https://eprint.iacr.org/2022/1664.pdf>

❖ **Gen(1^λ)**

- ◆ $(pk, sk) = \text{Gen}(1^\lambda)$
 - $f', g \leftarrow \psi_1^n$
 - $f = 3f' + 1$
 - check if f and g are invertible
 - $pk = 3gf^{-1}, sk = f$

❖ **Enc($pk, m \leftarrow \psi_1^n; r \leftarrow \psi_1^n$)**

- ◆ $c = hr + m$

❖ **Dec(sk, c)**

- ◆ $m = (cf \bmod q) \bmod^{\pm} 3$

❖ **Recover^r(h, c, m)**

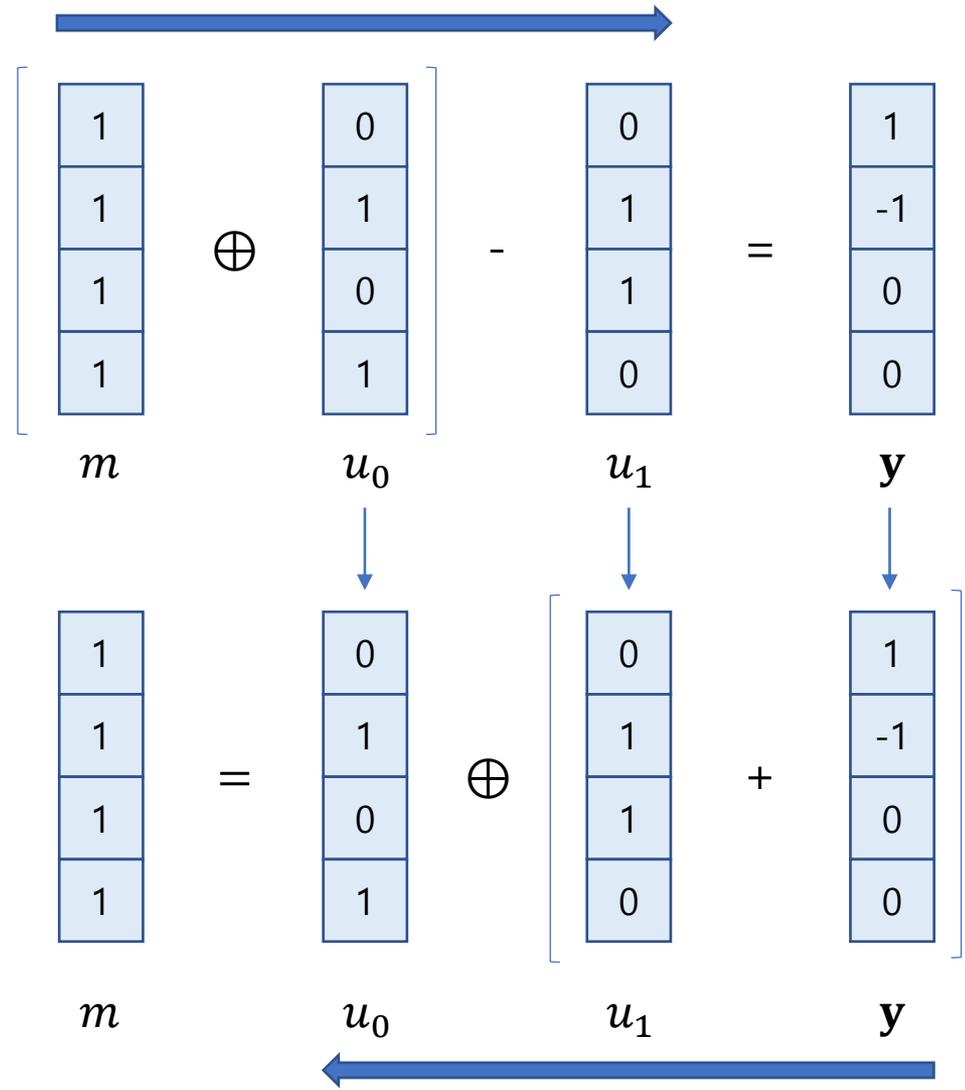
- ◆ $r = (c - m)h^{-1}$

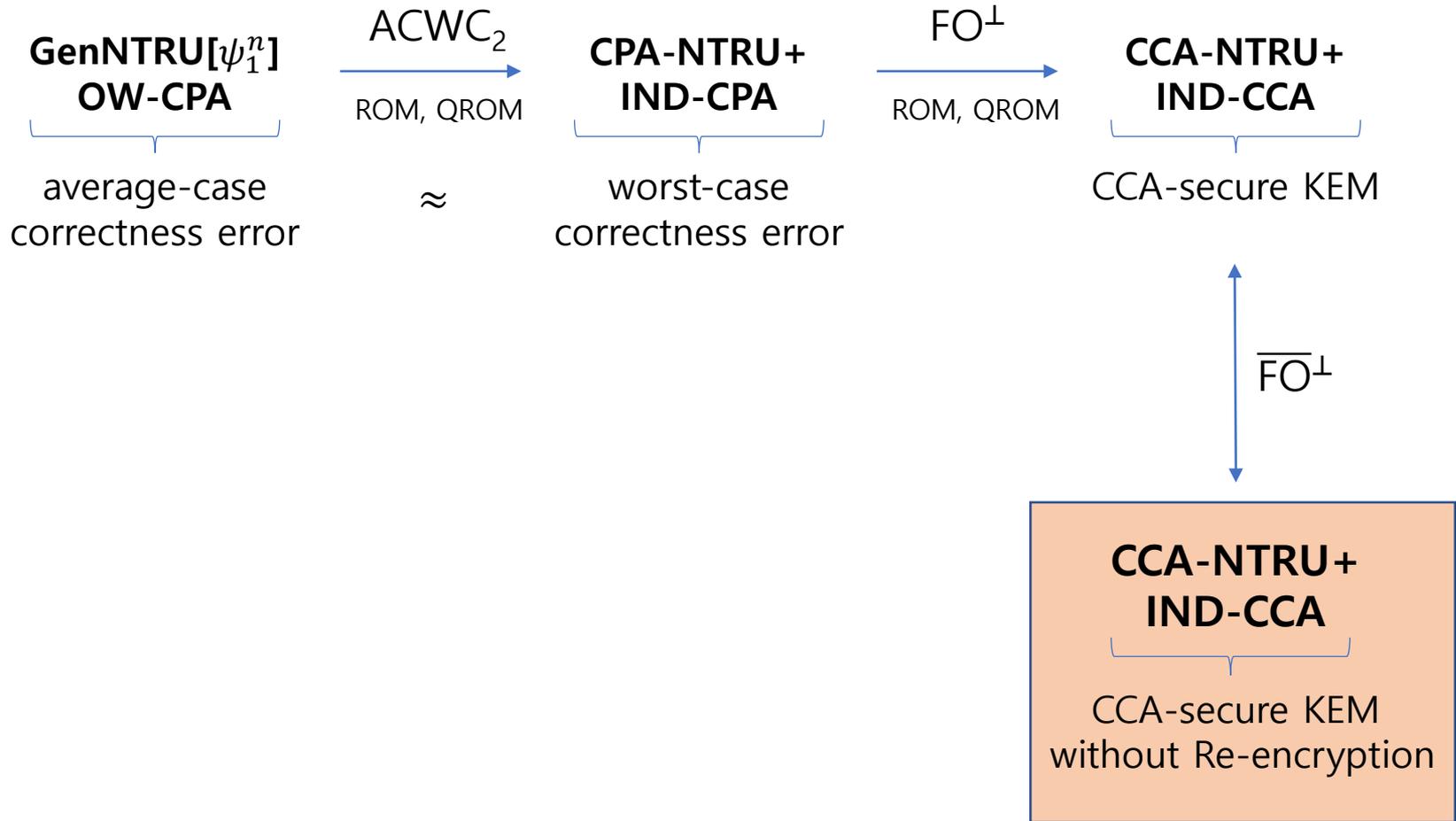
❖ SOTP(m, u)

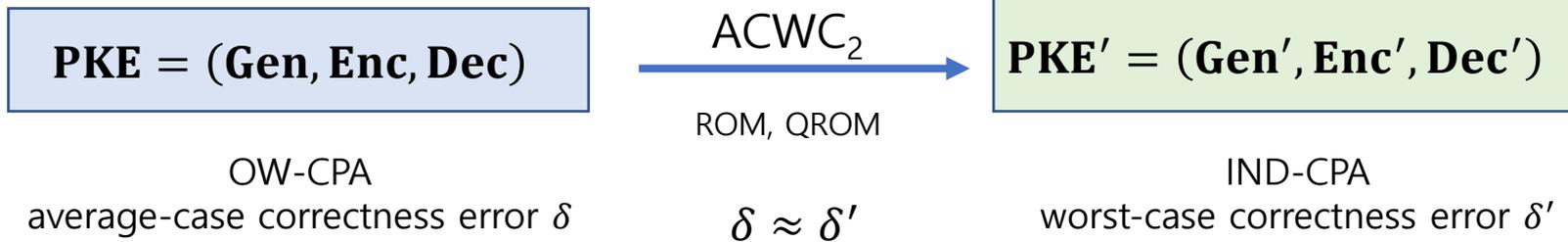
- ◆ $m \in \{0,1\}^n$
- ◆ $u = (u_0, u_1) \in \{0,1\}^{2n}$
- ◆ return $y = (m \oplus u_0) - u_1$

❖ Inv(y, u)

- ◆ $u = (u_0, u_1) \in \{0,1\}^{2n}$
- ◆ $m = (y + u_1) \oplus u_0$
- ◆ return $m \in \{0,1\}^n$





❖ ACWC₂ Transform [KP22]◆ **Gen'**(1^λ)

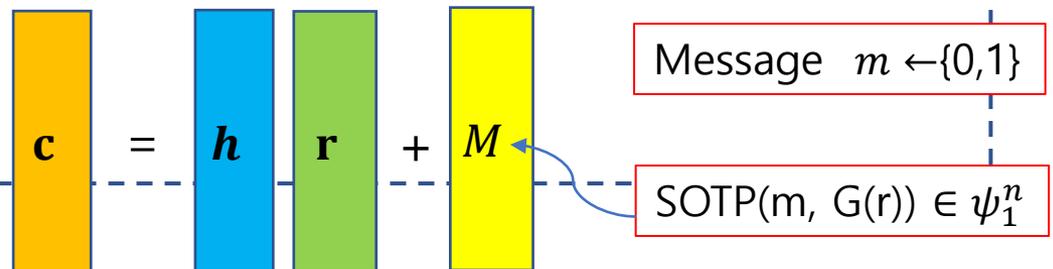
- $(pk, sk) = \mathbf{Gen}(1^\lambda)$
- **return** (pk, sk)

◆ **Enc'**($pk, m \in \mathcal{M}'$; $r \leftarrow \psi_1^n$)

- $M = \mathbf{SOTP}(m, G(r))$
- $c = \mathbf{Enc}(pk, M; r)$
- **return** c

◆ **Dec'**(sk, c)

- $M = \mathbf{Dec}(sk, c)$
- $r = \mathbf{Recover}^r(pk, M, c)$
- $m = \mathbf{Inv}(M, G(r))$
- **return** m



❖ **Gen'**(1^λ)

- ◆ $(pk, sk) = \mathbf{Gen}(1^\lambda)$
 - $\mathbf{f}', \mathbf{g} \leftarrow \psi_1^n$
 - $\mathbf{f} = 3\mathbf{f}' + \mathbf{1}$
 - check if \mathbf{f} and \mathbf{g} are invertible
 - $(pk, sk) = (3\mathbf{g}\mathbf{f}^{-1}, \mathbf{f})$

❖ **Enc'**($pk, m; \mathbf{r} \leftarrow \psi_1^n$)

- ◆ $\mathbf{m} = \mathbf{SOTP}(m, \mathbf{G}(\mathbf{r}))$
 - $(u_0, u_1) = \mathbf{G}(\mathbf{r})$
 - $\mathbf{m} = (m \oplus u_0) - u_1$

- ◆ $\mathbf{c} = \mathbf{Enc}(\mathbf{h}, \mathbf{m}; \mathbf{r})$
 - $\mathbf{c} = \mathbf{hr} + \mathbf{m}$

❖ **Dec'**(sk, \mathbf{c})

- ◆ $\mathbf{m}' = \mathbf{Dec}(\mathbf{f}, \mathbf{c})$
 - $\mathbf{m}' = (\mathbf{c}\mathbf{f} \bmod q) \bmod^{\pm} 3$

- ◆ $\mathbf{r}' = \mathbf{Recover}^r(\mathbf{h}, \mathbf{c}, \mathbf{m}')$
 - $\mathbf{r}' = (\mathbf{c} - \mathbf{m}')\mathbf{h}^{-1}$

- ◆ $m = \mathbf{Inv}(\mathbf{m}', \mathbf{G}(\mathbf{r}'))$
 - $(u_0, u_1) = \mathbf{G}(\mathbf{r}')$
 - $m = (\mathbf{m}' + u_1) \oplus u_0$

❖ **KeyGen**(1^λ)

- ◆ $(pk, sk) = \mathbf{Gen}(1^\lambda)$
 - $\mathbf{f}', \mathbf{g} \leftarrow \psi_1^n$
 - $\mathbf{f} = 3\mathbf{f}' + \mathbf{1}$
 - check if \mathbf{f} and \mathbf{g} are invertible
 - $(pk, sk) = (3\mathbf{g}\mathbf{f}'^{-1}, \mathbf{f})$

❖ **Encap**

- ◆ $m \leftarrow \{0,1\}^n$
- ◆ $(K, \mathbf{r}) = \mathbf{H}(m)$
- ◆ $\mathbf{c} = \mathbf{Enc}'(pk, m; \mathbf{r})$
 - $\mathbf{m} = \mathbf{SOTP}(m, \mathbf{G}(\mathbf{r}))$
 - $\mathbf{c} = \mathbf{Enc}(\mathbf{h}, \mathbf{m}; \mathbf{r})$

❖ **Decap**

- ◆ $\mathbf{m}' = \mathbf{Dec}'(sk, \mathbf{c})$
 - $\mathbf{m}' = \mathbf{Dec}(\mathbf{f}, \mathbf{c})$
 - $\mathbf{r}' = \mathbf{Recover}^r(\mathbf{h}, \mathbf{c}, \mathbf{m}')$
 - $\mathbf{m}' = \mathbf{Inv}(\mathbf{m}', \mathbf{G}(\mathbf{r}'))$
- ◆ $(K', \mathbf{r}'') = \mathbf{H}(m')$
- ◆ If $\mathbf{c} = \mathbf{Enc}'(pk, m'; \mathbf{r}'')$
 - Return K'
 - Else, return \perp

❖ **KeyGen**(1^λ)

- ◆ $(pk, sk) = \mathbf{Gen}(1^\lambda)$
 - $\mathbf{f}', \mathbf{g} \leftarrow \psi_1^n$
 - $\mathbf{f} = 3\mathbf{f}' + \mathbf{1}$
 - check if \mathbf{f} and \mathbf{g} are invertible
 - $(pk, sk) = (3\mathbf{g}\mathbf{f}^{-1}, \mathbf{f})$

❖ **Encap**

- ◆ $m \leftarrow \{0,1\}^n$
- ◆ $(K, \mathbf{r}) = \mathbf{H}(m)$
- ◆ $\mathbf{c} = \mathbf{Enc}'(pk, m; \mathbf{r})$
 - $\mathbf{m} = \mathbf{SOTP}(m, \mathbf{G}(\mathbf{r}))$
 - $\mathbf{c} = \mathbf{Enc}(\mathbf{h}, \mathbf{m}; \mathbf{r})$

❖ **Decap**

- ◆ $\mathbf{m}' = \mathbf{Dec}'(sk, \mathbf{c})$
 - $\mathbf{m}' = \mathbf{Dec}(\mathbf{f}, \mathbf{c})$
 - $\mathbf{r}' = \mathbf{Recover}^r(\mathbf{h}, \mathbf{c}, \mathbf{m}')$
 - $\mathbf{m}' = \mathbf{Inv}(\mathbf{m}', \mathbf{G}(\mathbf{r}'))$
- ◆ $(K', \mathbf{r}'') = \mathbf{H}(m')$
- ◆ If $\mathbf{r}' == \mathbf{r}''$
 - Return K'
 - Else, return \perp

❖ Ring Structure

$$\diamond R_q = \mathbb{Z}_q[x]/\langle \Phi_{3n}(x) \rangle$$

▪ $\Phi_{3n}(x) = x^n - x^{n/2} + 1$: $3n$ -th cyclotomic polynomial

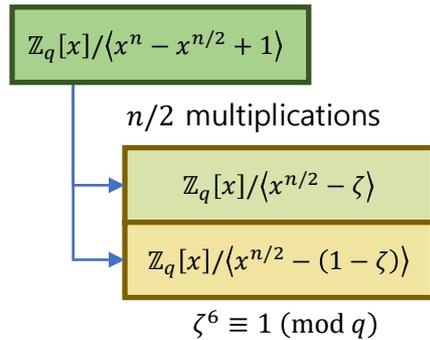
• $n = 2^i 3^j$

» $n = 512, \mathbf{576}, 648, \mathbf{768}, \mathbf{864}, 972, 1024, \mathbf{1152}, \dots$

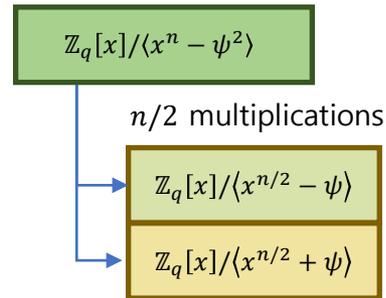
	Sec. level	n	q	PK (Byte)	CT (Byte)	SK (Byte)	Dec. Failure	Classical (Core-SVP)		Quantum (Core-SVP)	
								Primal	Dual	Primal	Dual
NTRU+ 576	1	576	3457	864	864	1,728	2^{-487}	116	115	105	104
NTRU+ 768	1+	768		1,152	1,152	2,304	2^{-379}	163	161	148	146
NTRU+ 864	3	864		1,296	1,296	2,592	2^{-340}	191	188	173	171
NTRU+ 1152	5	1152		1,728	1,728	3,456	2^{-260}	269	264	244	240

Algorithm	sec. (c)	n	q	PK (Byte)	CT (Byte)	SK (Byte)	$\log_2 \delta$	Reference (K Cycles)			AVX2 (K Cycles)		
								Gen	Encap	Decap	Gen	Encap	Decap
NTRU+ 576	115	576	3,457	864	864	1,728	-487	321	111	163	17	14	12
NTRU+ 768	161	768		1,152	1,152	2,304	-379	314	146	227	16	18	16
NTRU+ 864	188	864		1,296	1,296	2,592	-340	340	170	262	14	19	18
NTRU+ 1152	264	1,152		1,728	1,728	3,456	-260	905	230	348	43	26	24
Kyber 512	117	256x2	3,329	800	768	1,632	-139	100	126	152	26	35	26
Kyber 768	181	256x3		1,184	1,088	2,400	-164	179	210	245	43	54	42
Kyber 1024	253	256x4		1,568	1,568	3,168	-174	275	308	351	59	78	63
NTRUHPS 2048509	106	509	2,048	699	699	935	$-\infty$	7,808	586	1,424	191	80	33
NTRUHRSS 701	136	701	8,192	1,138	1,138	1,450	$-\infty$	15,190	3,821	11,191	251	58	51
NTRUHPS 2048677	145	677	2,048	930	930	1,234	$-\infty$	13,283	1,043	2,624	298	109	48
NTRUHPS 4096821	179	821	4096	1,230	1,230	1,590	$-\infty$	19,864	1,498	3,831	407	130	62

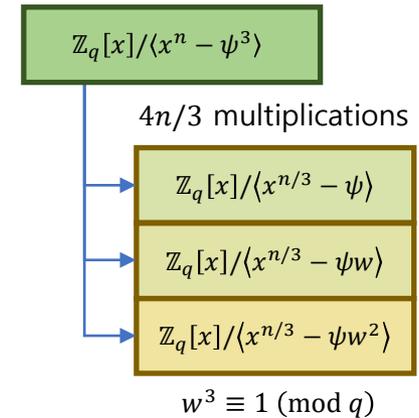
❖ Composition of NTT Layers



<Radix-2 NTT with trinomial Layer>

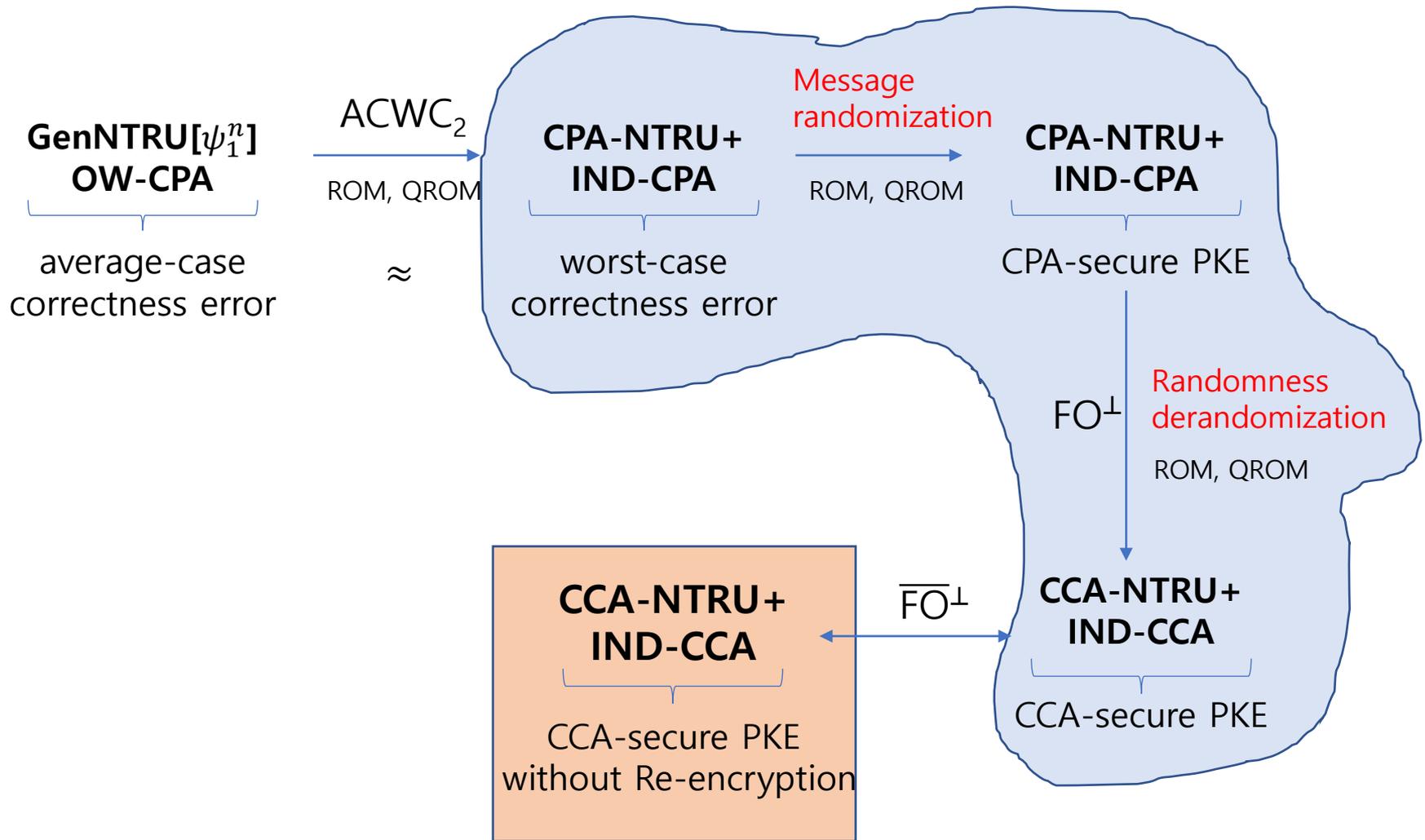


<Radix-2 NTT Layer>



<Radix-3 NTT Layer>

	n	q	Radix-2 NTT with trinomial	Radix-3 NTT	Radix-2 NTT	Inertia degree
NTRU+576	576	3457	1	2	4	2
NTRU+768	768		1	1	4	2
NTRU+864	864		1	2	4	3
NTRU+1152	1152		1	2	5	2



Thank You

Q&A