NTRU+

Compact Construction of NTRU Using Simple Encoding Method

2023.05.18.

상명대학교

박 종 환

Contents

Ring over Polynomials

❖ Ring $R_q = Z_q[x]/f(x)$

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

❖ Ring $R_q = Z_q[x]/f(x) = \{a_0 + a_1 x + \cdots a_n x^{n-1} \mid a_i \in Z_q\}$

- Representation:

$$a(x) = a_0 + a_1 x + \cdots + a_n x^{n-1} \leftrightarrow (a_0, a_1, \ldots, a_{n-1}) \in (Z_q)^n$$
$$b(x) = b_0 + b_1 x + \cdots + b_n x^{n-1} \leftrightarrow (b_0, b_1, \ldots, b_{n-1}) \in (Z_q)^n$$

- Addition/subtraction:

$$(a_0, a_1, \ldots, a_{n-1}) \pm (b_0, b_1, \ldots, b_{n-1}) = (a_0 \pm b_0, a_1 \pm b_1, \ldots, a_{n-1} \pm b_{n-1})$$

- Multiplication:

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

- Division:

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

Using NTT

Ring Choice (1)

❖ Ring $R_q = Z_q[x]/f(x)$

- $f(x) = x^n + 1, \quad where \ n = 2^k$ - **KYBER, FALCON, Dillithium**
- $f(x) = x^n - 1, \quad where \ n$ is prime – **NTRU**

❖ $R_q = Z_q[x]/< x^n + 1 > \quad (n = 2^k)$

+ Easy to implement NTT
– Sparse $n = 256, 512, 1024, \ldots$

$Security(n = 512) < 128$
$Security(n = 1024) \gg 128$

❖ $R_q = Z_q[x]/< x^n - 1 >$ ($n =$ prime)

– Hard to implement NTT
+ Dense $n = 521, 523, 542, 547, 557, 563, 569, \ldots$

Ring Choice (2)

- Ring $R_q = Z_q[x]/f(x)$
  - $f(x) = x^n + 1, \quad where \ n = 2^k$ - **KYBER, FALCON, Dillithium**
  - $f(x) = x^n - 1, \quad where \ n$ is prime – **NTRU**
  - $f(x) = x^n - x^{\frac{n}{2}} + 1, \quad where \ n = 2^i 3^j$ – **NTRU+**

- $R_q = Z_q[x]/< x^n - x^{n/2} + 1 > (n = 2^i 3^j)$
  - \+ Easy to implement NTT [LS19]
  - \+ Moderate $n =$ **512**, 576, 648, 768, 864, 972, **1024,...**

[LS19] Lyubashevsky et al., "NTTRU: Truly Fast NTRU Using NTT", TCHES 2019

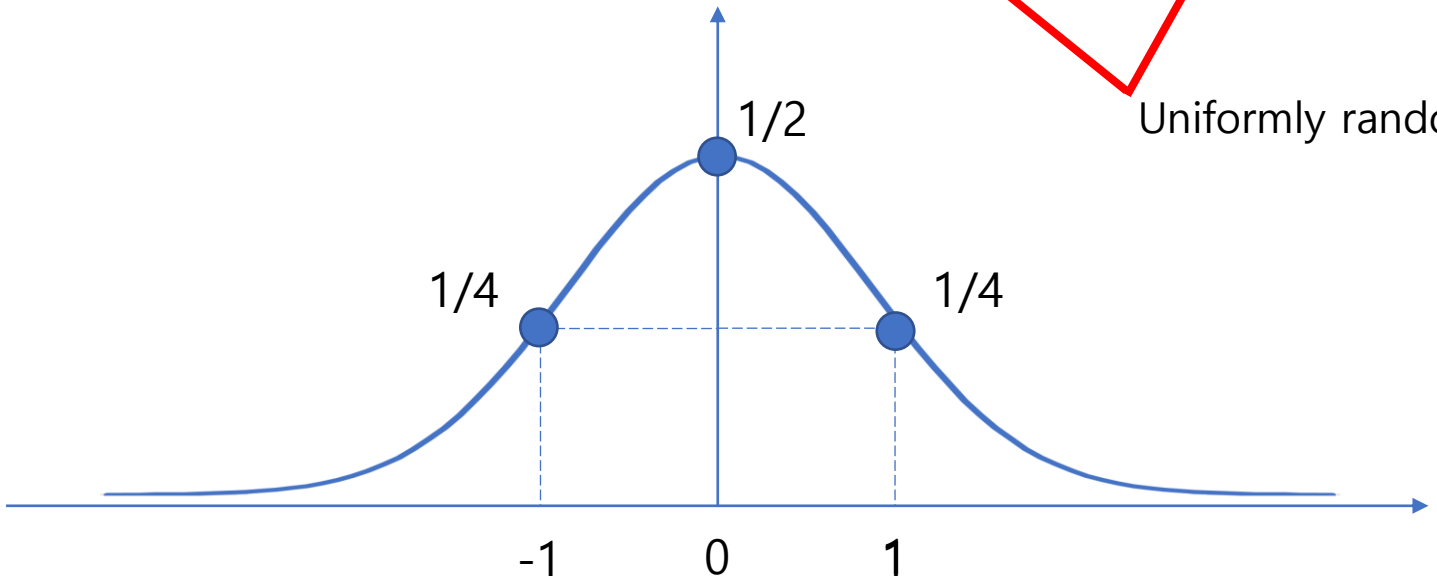
Centered Binomial Distribution (CBD)

❖ **CBD$_1(u)$**

- $u = (u_0, u_1) \leftarrow_u \{0,1\}^{2n}$
- **return** $y = u_0 - u_1$ (component-wise)

u_0	-	u_1	=	y
0		0		0
1		1		0
0		1		-1
1		0		1

Uniformly random bits



Correctness Error of PKE

- **PKE**
  - KeyGen → (pk, sk)
  - Enc(pk, m ; r) = C
  - Dec(sk, C) = m

- **Correctness: Dec(sk, Enc(pk, m ; r)) = m**
  - **Average-case correctness error**
    - $\Pr_{m \leftarrow \psi_{\mathcal{M}}, r \leftarrow \psi_{\mathcal{R}}}\left[Dec\left(sk, Enc(pk, m; r)\right) \neq m\right] \leq \delta$
  - **Worst-case correctness error**
    - $\Pr_{m \in \psi_{\mathcal{M}}, r \in \psi_{\mathcal{R}}}\left[Dec\left(sk, Enc(pk, m; r)\right) \neq m\right] \leq \delta$
  - **Perfect correctness error**
    - $\Pr_{\forall\, m \in \psi_{\mathcal{M}}, \forall\, r \in \psi_{\mathcal{R}}}\left[Dec\left(sk, Enc(pk, m; r)\right) \neq m\right] = 0$

NTRU Ring (1)

- **In a ring $R_q = Z_q[x] \,/\, (x^n - 1)$**
  - **(n, q) chosen and small prime $p = 3$**

- **Ring $R_q = \mathbb{Z}_q[x]/f(x) = \{a_0 + a_1 x + \cdots a_n x^{n-1} \mid a_i \in \mathbb{Z}_q\}$**
  - **Representation**

$$a(x) = a_0 + a_1 x + \cdots + a_n x^{n-1} \;\leftrightarrow\; (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q$$

- **Ring $R_p = \mathbb{Z}_p[x]/f(x) = \{a_0 + a_1 x + \cdots a_n x^{n-1} \mid a_i \in \mathbb{Z}_p\}$**
  - **Representation**

$$a(x) = a_0 + a_1 x + \cdots + a_n x^{n-1} \;\leftrightarrow\; (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$$

  - $p \ll q$

NTRU Ring (2)

❖ 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
  - $\boldsymbol{f} = 1 - x + x^3 - x^7 + \cdots + x^{504} - x^{508}$
  - $\boldsymbol{g} = 1 + x^2 - x^5 + x^{10} - \cdots - x^{506} - x^{507}$

$[-1, 1]$ in R_p

$[-1024, 1024]$ in R_q

  - $\boldsymbol{f_q^{-1}}$ (in R_q) $= -1011 + 488x + 964x^2 - 815x^3 - \cdots + 735x^{507} - 633x^{508}$
  - $\boldsymbol{f_p^{-1}}$ (in R_p) $= -1 + x + x^2 - x^3 - \cdots + x^{506} - x^{508}$
  - $\boldsymbol{h} = \boldsymbol{g} \cdot \boldsymbol{f_q^{-1}}$ (in R_q) $= -976 - 288x + 519x^2 + 852x^3 + \cdots - 1021x^{507} + 491x^{508}$

- Coefficients of (r, m) chosen in $[-1, 1]$ in R_p
  - $\boldsymbol{r} = -1 + x - x^2 - x^5 + \cdots + x^{506} + x^{508}$
  - $\boldsymbol{m} = 1 + x + x^4 - x^5 - \cdots + x^{506} - x^{507}$

$[-1, 1]$ in R_p

  - $\mathbf{c} = p\boldsymbol{h} \cdot \boldsymbol{r} + \boldsymbol{m}$ (in R_q) $= 277 + 993x + \cdots + 1001x^{507} - 388x^{508}$

NTRU PKE (1) [HPS98]

scalar multiplication

❖ $R_q = \mathbb{Z}_q[x]/< x^n - 1 >, \quad p = 3$

- **Public key :** $\boldsymbol{h} = p\,(\boldsymbol{g} \cdot \boldsymbol{f_q^{-1}}) \in R_q$ **Secret key :** $\boldsymbol{f}, \boldsymbol{f_p^{-1}}$
- **Ciphertext :** $\boldsymbol{c} = \boldsymbol{r} \cdot \boldsymbol{h} + \boldsymbol{m} \in R_q$

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

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

PK : $\boldsymbol{h} = \left[p \; \boldsymbol{g} \cdot \boldsymbol{f_q^{-1}} \right]_{R_q}$ SK : $\boldsymbol{f} \quad \boldsymbol{f_p^{-1}}$

CT : $\boldsymbol{c} = \left[\boldsymbol{r} \cdot \boldsymbol{h} + \boldsymbol{m} \right]_{R_q}$

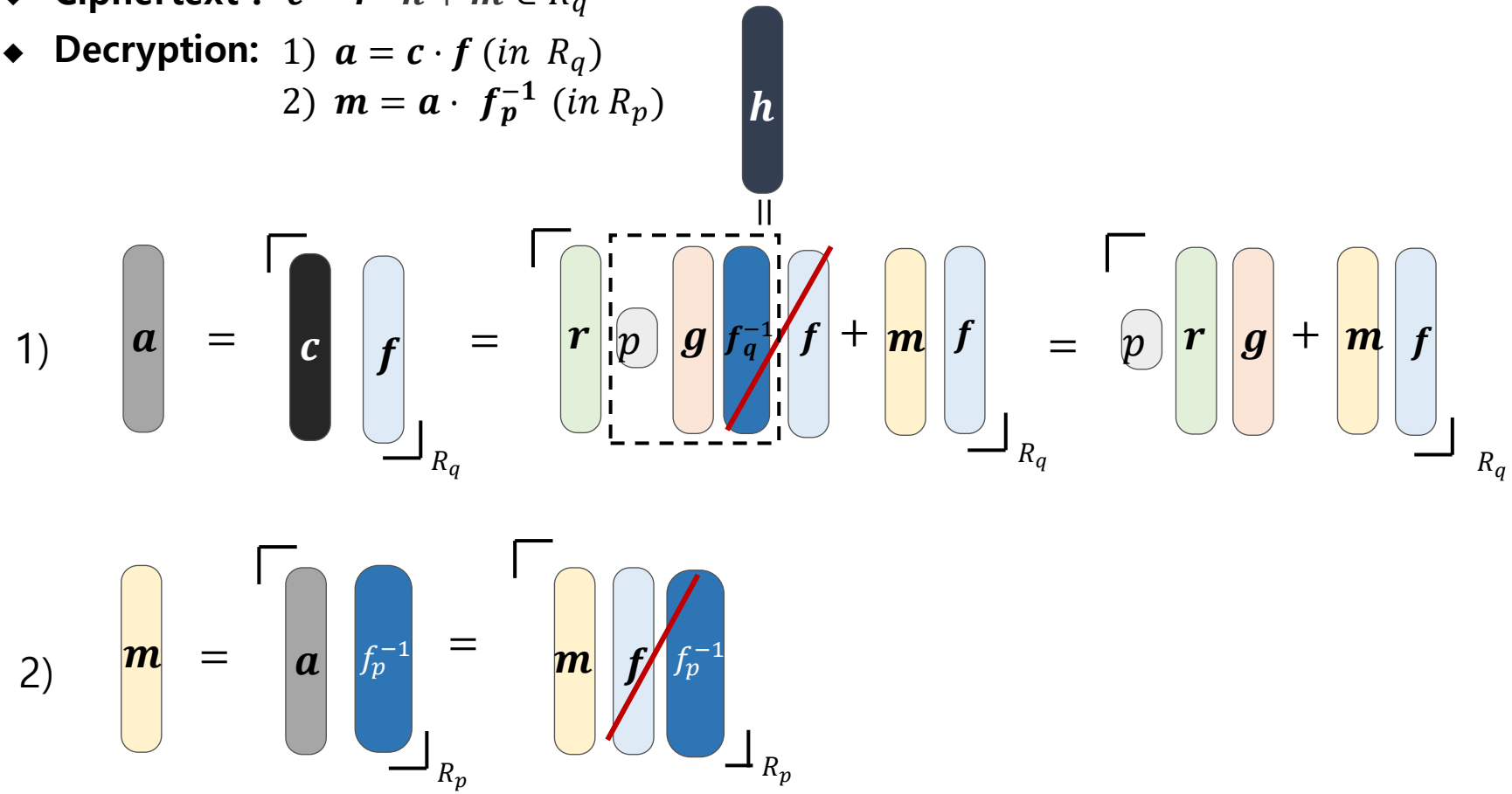
- $\mathcal{T}_{fixed-weight}$: fixed-weight ternary distribution (e.g., $n = 743, \; h = 494$)
- $\mathcal{T}_{uniform}$: uniform distribution among $\{-1,0,1\}$

[HPS98] Hoffstein et al., "NTRU: A ring-based public key cryptosystem", ANTS 1998

NTRU PKE (2)

❖ $R_q = \mathbb{Z}_q[x]/< x^n - 1 >,\ \ p = 3$

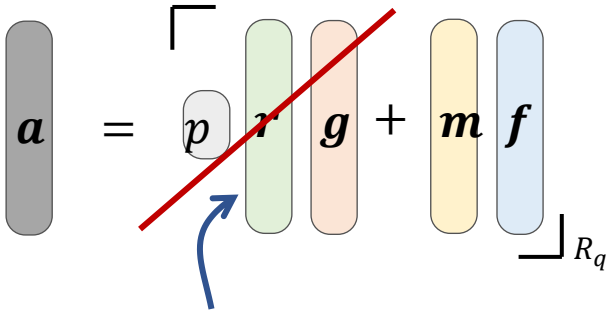
- **Public key :** $\boldsymbol{h} = p\,(\boldsymbol{g} \cdot \boldsymbol{f_q^{-1}}) \in R_q$ **Secret key :** $\boldsymbol{f}, \boldsymbol{f_p^{-1}}$
- **Ciphertext :** $\boldsymbol{c} = \boldsymbol{r} \cdot \boldsymbol{h} + \boldsymbol{m} \in R_q$
- **Decryption:** 1) $\boldsymbol{a} = \boldsymbol{c} \cdot \boldsymbol{f}\ (in\ R_q)$
  2) $\boldsymbol{m} = \boldsymbol{a} \cdot \boldsymbol{f_p^{-1}}\ (in\ R_p)$



NTRU PKE (3)

❖ $R_q = \mathbb{Z}_q[x]/< x^n - 1 >,\ \ p = 3$

- **Public key :** $\boldsymbol{h} = p\,(\boldsymbol{g} \cdot \boldsymbol{f_q^{-1}}) \in R_q$ **Secret key :** $\boldsymbol{f},\ \boldsymbol{f_p^{-1}}$
- **Ciphertext :** $\boldsymbol{c} = \boldsymbol{r} \cdot \boldsymbol{h} + \boldsymbol{m} \in R_q$
- **Decryption:** *1)* $\boldsymbol{a} = \boldsymbol{c} \cdot \boldsymbol{f}\ \ (in\ \ R_q)$
  2) $\boldsymbol{m} = \boldsymbol{a} \cdot \boldsymbol{f_p^{-1}}\ \ (in\ R_p)$
  - Decryption works only when all coefficients of $\boldsymbol{a} = p(\boldsymbol{r} \cdot \boldsymbol{g}) + \boldsymbol{m} \cdot \boldsymbol{f}\ \in [-q/2,\ q/2]$



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

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

NTRU PKE (4) - Variant

❖ $R_q = \mathbb{Z}_q[x]/< x^n - 1 >,\ \ p = 3$

- **Public key :** $\boldsymbol{h} = p\,(\boldsymbol{g} \cdot \boldsymbol{f}^{-1}) \in R_q$ **Secret key :** $\boldsymbol{f}$
  - $\boldsymbol{f} = 3\boldsymbol{f}' + 1$, where $\boldsymbol{f}'$ chosen in R_p
- **Ciphertext :** $\boldsymbol{c} = \boldsymbol{r} \cdot \boldsymbol{h} + \boldsymbol{m} \in R_q$

$f = 3f' + 1$

PK : $\boldsymbol{h} = \lceil p\ \boldsymbol{g} \cdot \boldsymbol{f}^{-1} \rfloor_{R_q}$ SK : $\boldsymbol{f}$

CT : $\boldsymbol{c} = \lceil \boldsymbol{r} \cdot \boldsymbol{h} + \boldsymbol{m} \rfloor_{R_q}$

- Coefficients of f' are chosen from D_f,

NTRU PKE (5) - Variant

❖ $R_q = \mathbb{Z}_q[x]/< x^n - 1 >,\ \ p = 3$

- **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:** $m = c \cdot f\ (in\ R_q)\ (\mathrm{mod}\ p)$

$f = 3f' + 1$

$$m = \lfloor c\ f \rfloor_{R_q} = \lfloor r\ p\ g\ f^{-1}\ f + m\ f \rfloor_{R_q} = \lfloor p\ r\ g + m\ f \rfloor_{R_q}$$

$$= \lfloor p\ r\ g + p\ m\ f' + m \rfloor_{R_q}$$

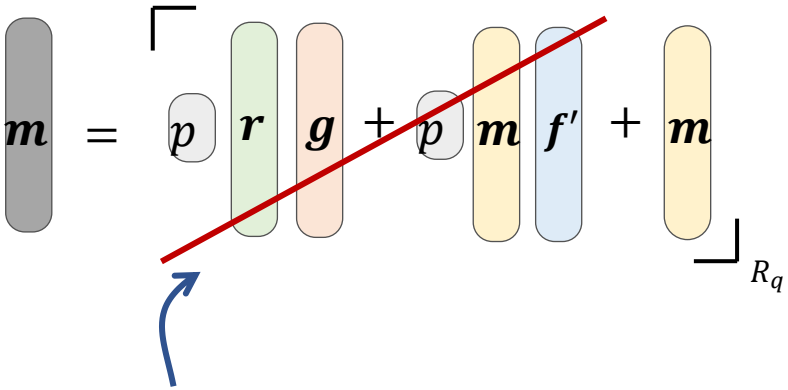
NTRU PKE (6) - Variant

❖ $R_q = \mathbb{Z}_q[x]/< x^n - 1 >,\ \ p = 3$

- **Public key :** $\boldsymbol{h} = p\,(\boldsymbol{g} \cdot \boldsymbol{f}^{-1}) \in R_q$ **Secret key :** $\boldsymbol{f}$
  - $\boldsymbol{f} = 3\boldsymbol{f}' + 1$, where $\boldsymbol{f}'$ chosen in R_p
- **Ciphertext :** $\boldsymbol{c} = \boldsymbol{r} \cdot \boldsymbol{h} + \boldsymbol{m} \in R_q$
- **Decryption:** $\boldsymbol{m} = \boldsymbol{c} \cdot \boldsymbol{f}\ (in\ R_q)\ (\mathrm{mod}\ p)$

$$f = 3f' + 1$$

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



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

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

Correctness Issue of NTRU (1)

❖ Correctness error of NTRU

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

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

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

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

Decryption Oracle

$\mathbf{c}$ ←

→ $\mathbf{m}'$

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

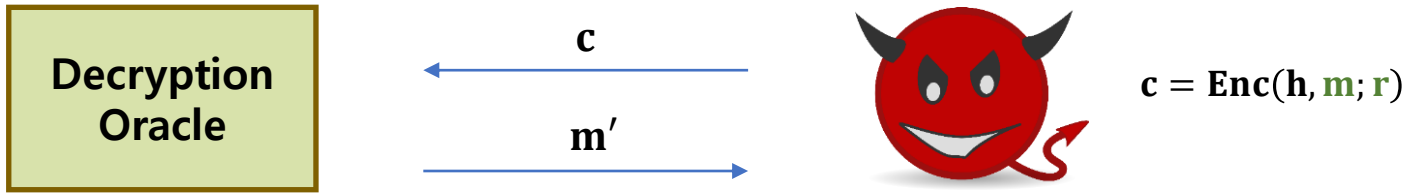
If $\mathbf{m} \neq \mathbf{m}'$,

$$\|p(\mathbf{gr}+\mathbf{mf}')+\mathbf{m}\|_\infty \geq \frac{q}{2}$$

➔leakage about $\mathbf{g}$ and $\mathbf{f}'$

Correctness Issue of NTRU (2)

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



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

- $H(m) = r$
- $c = Enc(pk, m; r)$

Fortunately,
It is **hard** to control r=($\boldsymbol{r}, \boldsymbol{e_1}, \boldsymbol{e_2}$) when FO transform is applied

◆ Average-case correctness error ≈ worst-case correctness error

[HHK17] Hofheinz et al., "A Modular Analysis of the Fujisaki-Okamoto Transformation", TCC 2017

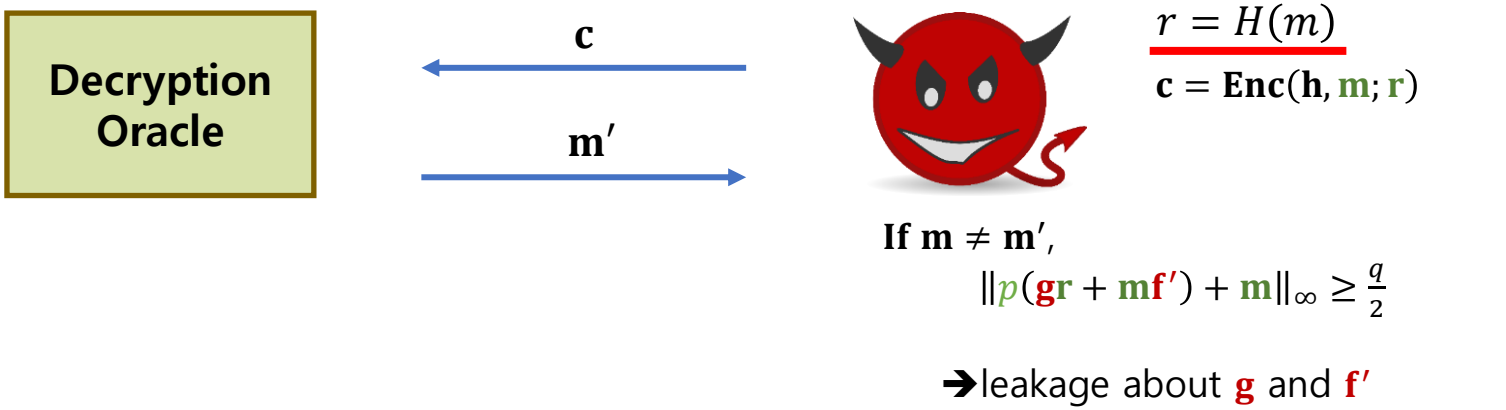
Correctness Issue of NTRU (3)

❖ Correctness error of NTRU

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

❖ When using FO-transform

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



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

Correctness Issue of NTRU (4)

❖ How to achieve worst-case correctness error

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

- **Solution 1 – <u>perfect correctness error</u>**
  - All (m, r) tuples do not make NTRU decryption fail
  - Require modulus q to be relatively large
  - Need to check if (m, r) are well-formed in decryption
  - Adopted by **Finalist NTRU**

- **Solution 2 - <u>worst-case correctness error</u>**
  - 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

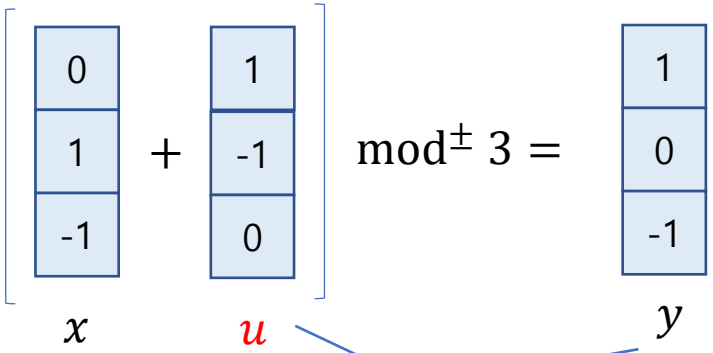
ACWC Transform - GOTP

❖ Generalized One-time Pad (GOTP)

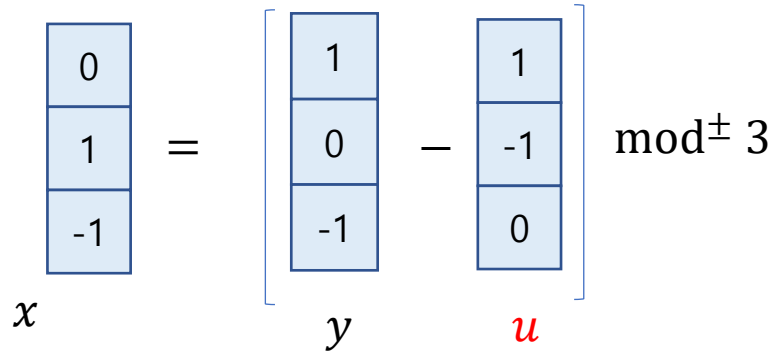
- U_3 distribution: uniformly random over {-1, 0, 1}
- $u \leftarrow U_3^n$

❖ GOTP for NTRU-B [DHK+21]

- **GOTP**$(x, u) = y$
  - $y = x + u \pmod{\pm 3}$



- **Inv**$(y, u) = x \in \{-1,0,1\}^n$
  - $x = y - u \pmod{\pm 3}$

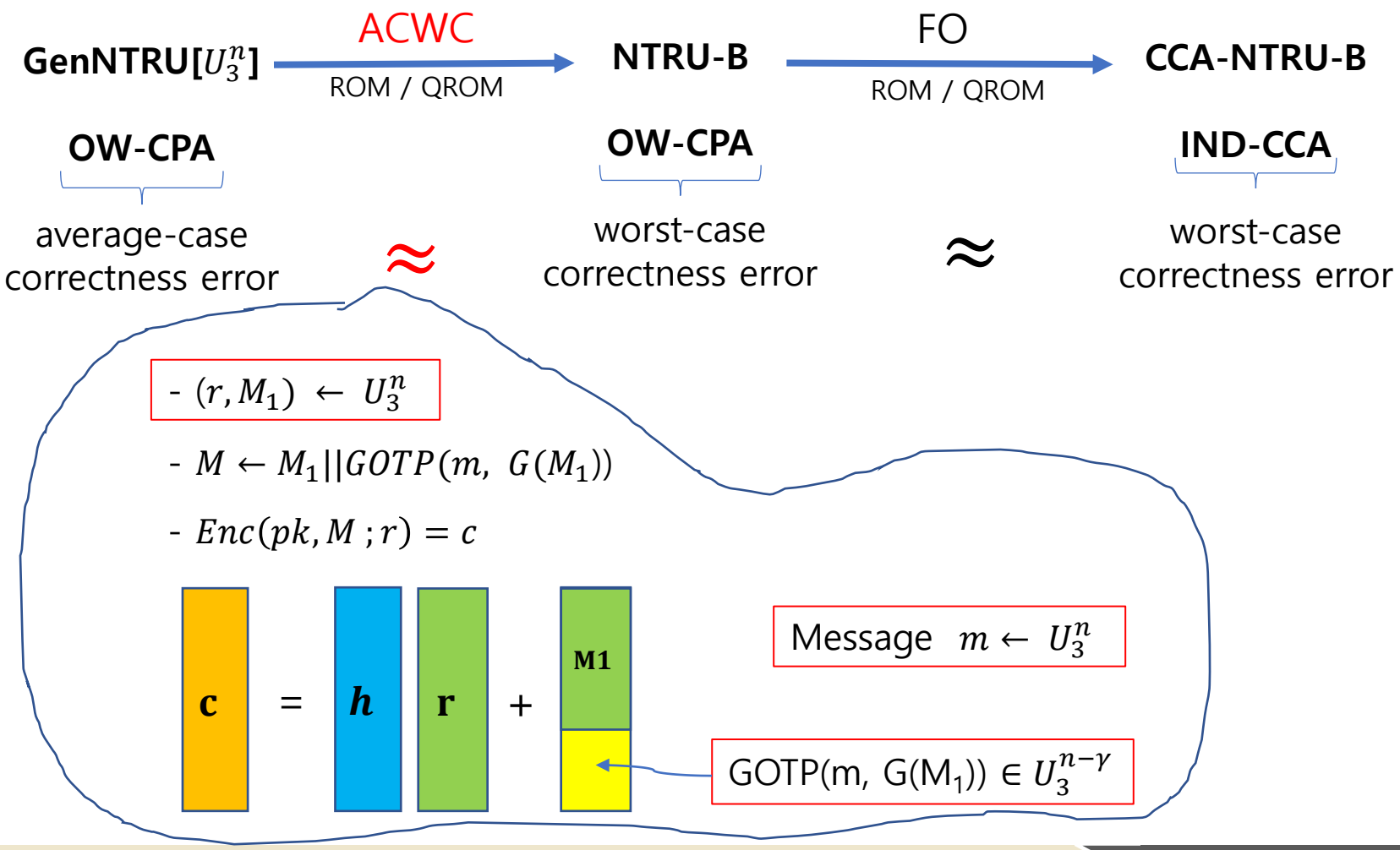


[DHK+21] Duman et al. "A Thorough Treatment of Highly-Efficient NTRU Instantiations", https://eprint.iacr.org/2021/1352.pdf

ACWC Transform

❖ ACWC transform [DHK+21]

- ◆ **GenNTRU[U_3^n]**
  - ▪ **(f, g, M, r) are sampled uniformly at random over $\{-1, 0, 1\}$**



Comparison to Previous NTRU Constructions

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	$\mathrm{ACWC} + \mathrm{FO}^\perp$	$\mathrm{ACWC}_2 + \overline{\mathrm{FO}}^\perp$
Assumptions	NTRU, RLWE	NTRU, RLWE	NTRU, RLWE
(classical) 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

GenNTRU[ψ_1^n]

- **Gen**(1^λ)
  - $(pk, sk) = \mathbf{Gen}(1^\lambda)$
    - $\mathbf{f}', \mathbf{g} \leftarrow \boldsymbol{\psi_1^n}$
    - $\mathbf{f} = 3\mathbf{f}' + 1$
    - check if $\mathbf{f}$ and $\mathbf{g}$ are invertible
    - $\boldsymbol{pk} = \boldsymbol{h} = 3\mathbf{g}\mathbf{f}^{-1}$, $\boldsymbol{sk} = \boldsymbol{f}$
- **Enc**$(\boldsymbol{pk}, \boldsymbol{m} \leftarrow \boldsymbol{\psi_1^n}; \mathbf{r} \leftarrow \boldsymbol{\psi_1^n})$
  - $\mathbf{c} = \mathbf{h}\mathbf{r} + \mathbf{m}$
- **Dec**$(\mathbf{sk}, \mathbf{c})$
  - $\boldsymbol{m} = (\mathbf{c}\mathbf{f} \bmod q) \bmod^{\pm} 3$

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

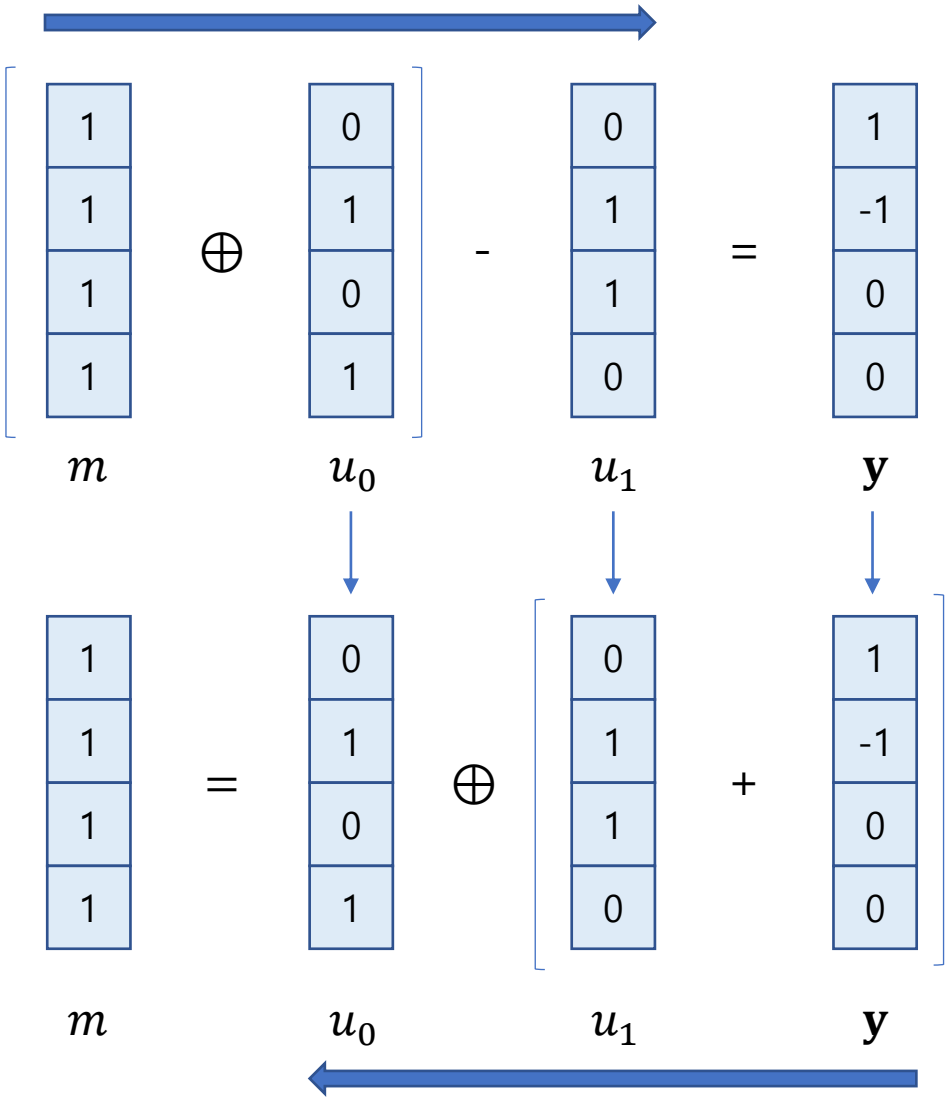
Semi-generalized OTP (SOTP)

❖ **SOTP**(m, u)

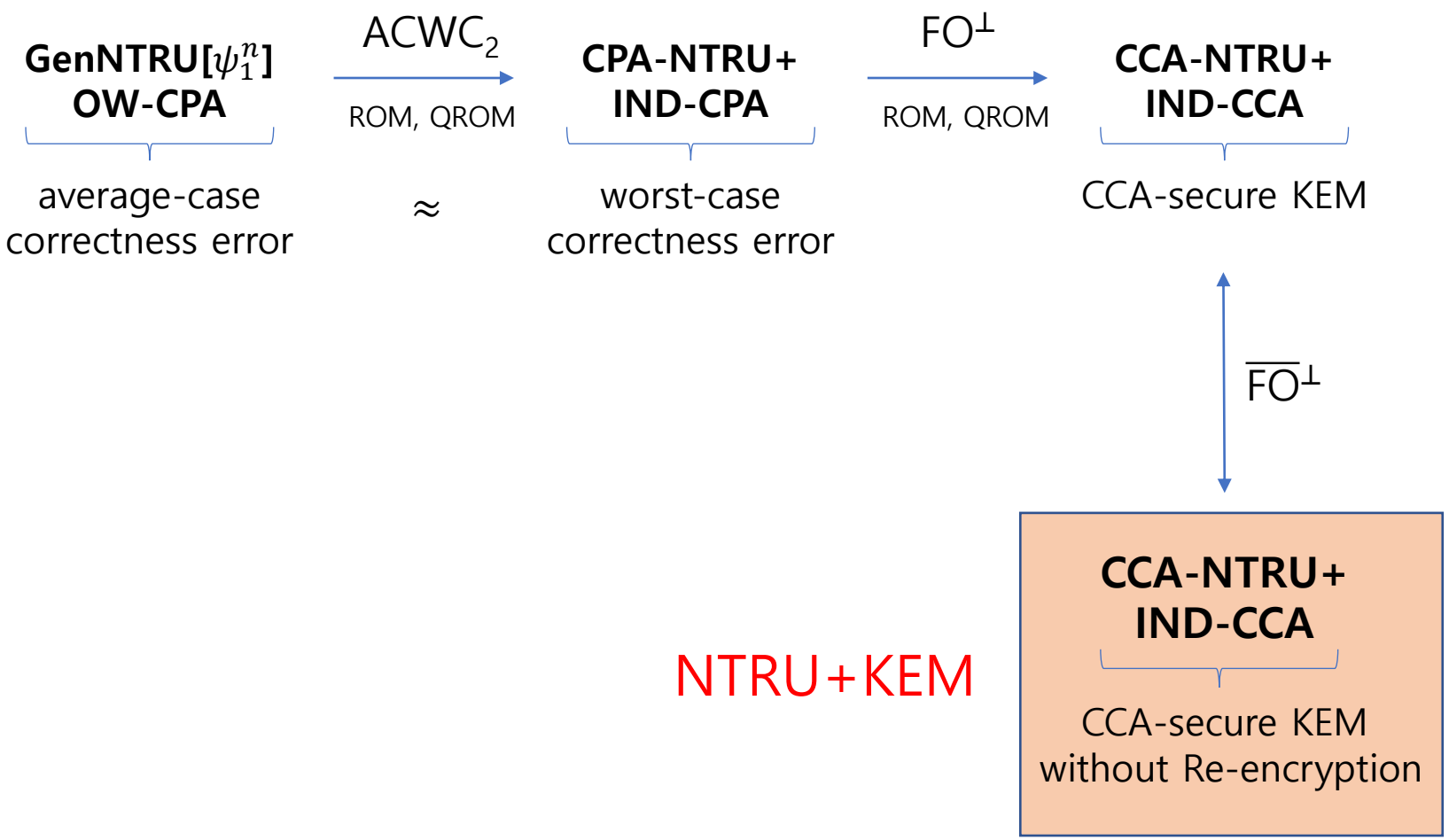
- $m \in \{0,1\}^n$
- $u = (u_0, u_1) \in \{0,1\}^{2n}$
- **return** $\mathbf{y} = (m \oplus u_0) - u_1$

❖ **Inv**(y, u)

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



Construction Overview



$ACWC_2$ Transform

❖ $ACWC_2$ Transform [KP22]

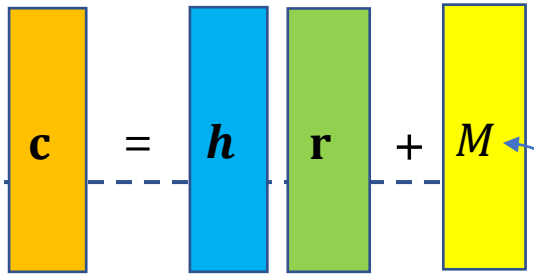
$\mathbf{PKE} = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$ —$ACWC_2$ (ROM, QROM)→ $\mathbf{PKE}' = (\mathbf{Gen}', \mathbf{Enc}', \mathbf{Dec}')$

OW-CPA
average-case correctness error δ

$\delta \approx \delta'$

IND-CPA
worst-case correctness error δ'

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



Message $m \leftarrow \{0,1\}^n$

SOTP(m, G(r)) $\in \psi_1^n$

CPA-NTRU+ from $ACWC_2$

❖ $\mathbf{Gen}'(1^\lambda)$

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

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

- $\mathbf{m} = \mathbf{SOTP}(m, \mathbf{G}(\mathbf{r}))$
  - $(u_0, u_1) = \mathbf{G}(\mathbf{r})$
  - $\mathbf{m} = (m \oplus u_0) - u_1$
- $\mathbf{c} = \mathbf{Enc}(\mathbf{h}, \mathbf{m}; \mathbf{r})$
  - $\mathbf{c} = \mathbf{h}\mathbf{r} + \mathbf{m}$

❖ $\mathbf{Dec}'(sk, \mathbf{c})$

- $\boldsymbol{m}' = \mathbf{Dec}(\mathbf{f}, \mathbf{c})$
  - $\boldsymbol{m}' = (\mathbf{c}\mathbf{f} \bmod q) \bmod^{\pm} 3$
- $\mathbf{r}' = \mathbf{Recover}^r(\mathbf{h}, \mathbf{c}, \mathbf{m}')$
  - $\boldsymbol{r}' = (\boldsymbol{c} - \boldsymbol{m}')\mathbf{h}^{-1}$
- $m = \mathbf{Inv}(\boldsymbol{m}', \mathbf{G}(\boldsymbol{r}'))$
  - $(u_0, u_1) = \mathbf{G}(\mathbf{r}')$
  - $m = (\mathbf{m}' + u_1) \oplus u_0$

CCA-NTRU+ from $\mathbf{FO}^{\perp}$

❖ KeyGen(1^{λ})

- $(pk, sk) = \mathbf{Gen}(1^{\lambda})$
  - $\mathbf{f}', \mathbf{g} \leftarrow \boldsymbol{\psi}_1^{\boldsymbol{n}}$
  - $\mathbf{f} = \mathbf{3f}' + \mathbf{1}$
  - check if $\mathbf{f}$ and $\mathbf{g}$ are invertible
  - $(pk, sk) = \left(\mathbf{h} = 3\mathbf{g}\mathbf{f}^{-1}, \mathbf{f}\right)$

❖ Encap

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

❖ Decap

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

CCA-NTRU+ from $\overline{\mathbf{FO}}^{\perp}$

❖ KeyGen(1^{λ})

- $(pk, sk) = \mathbf{Gen}(1^{\lambda})$
  - $\mathbf{f}', \mathbf{g} \leftarrow \boldsymbol{\psi}_1^{\boldsymbol{n}}$
  - $\mathbf{f} = \mathbf{3f}' + \mathbf{1}$
  - check if $\mathbf{f}$ and $\mathbf{g}$ are invertible
  - $(pk, sk) = \left(\mathbf{h} = 3\mathbf{g}\mathbf{f}^{-1}, \mathbf{f}\right)$

❖ Encap

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

❖ Decap

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

Parameters

❖ Ring Structure

- $R_q = \mathbb{Z}_q[x]/\langle \Phi_{3n}(x) \rangle$
  - $\Phi_{3n}(x) = x^n - x^{n/2} + 1$: $3n$-th cyclotomic polynomial
    - $n = 2^i 3^j$
      - » $n = 512, \mathbf{576}, 648, \mathbf{768}, \mathbf{864}, 972, 1024, \mathbf{1152}, \cdots$

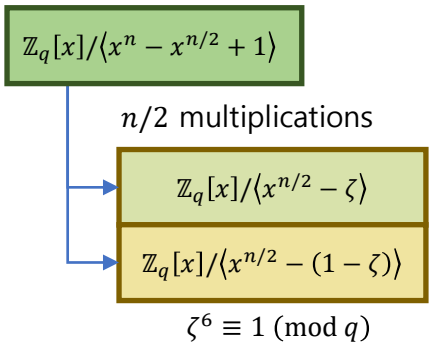
	Sec. level	n	q	PK (Byte)	CT (Byte)	SK (Byte)	Dec. Failure	Classical (Core-SVP)		Quantum (Core-SVP)	
								Primal	Dual	Primal	Dual
NTRU+ 576	1	576	3457	864	864	1,728	2^{-487}	116	115	105	104
NTRU+ 768	1+	768		1,152	1,152	2,304	2^{-379}	163	161	148	146
NTRU+ 864	3	864		1,296	1,296	2,592	2^{-340}	191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

Performance Analysis

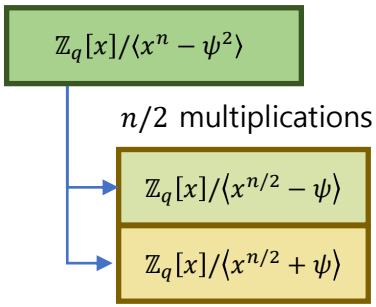
Algorithm	sec. (c)	n	q	PK (Byte)	CT (Byte)	SK (Byte)	$\log_2 \delta$	Reference (K Cycles)			AVX2 (K Cycles)		
								Gen	Encap	Decap	Gen	Encap	Decap
NTRU+ 576	115	576	3,457	864	864	1,728	-487	321	111	163	17	14	12
NTRU+ 768	161	768		1,152	1,152	2,304	-379	314	146	227	16	18	16
NTRU+ 864	188	864		1,296	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	-∞	7,808	586	1,424	191	80	33
NTRUHRSS 701	136	701	8,192	1,138	1,138	1,450	-∞	15,190	3,821	11,191	251	58	51
NTRUHPS 2048677	145	677	2,048	930	930	1,234	-∞	13,283	1,043	2,624	298	109	48
NTRUHPS 4096821	179	821	4096	1,230	1,230	1,590	-∞	19,864	1,498	3,831	407	130	62

NTT Implementation

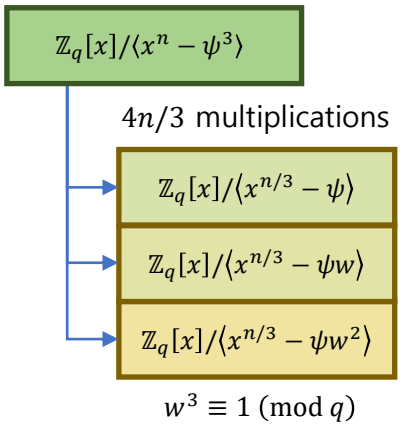
❖ Composition of NTT Layers



<Radix-2 NTT with trinomial Layer>



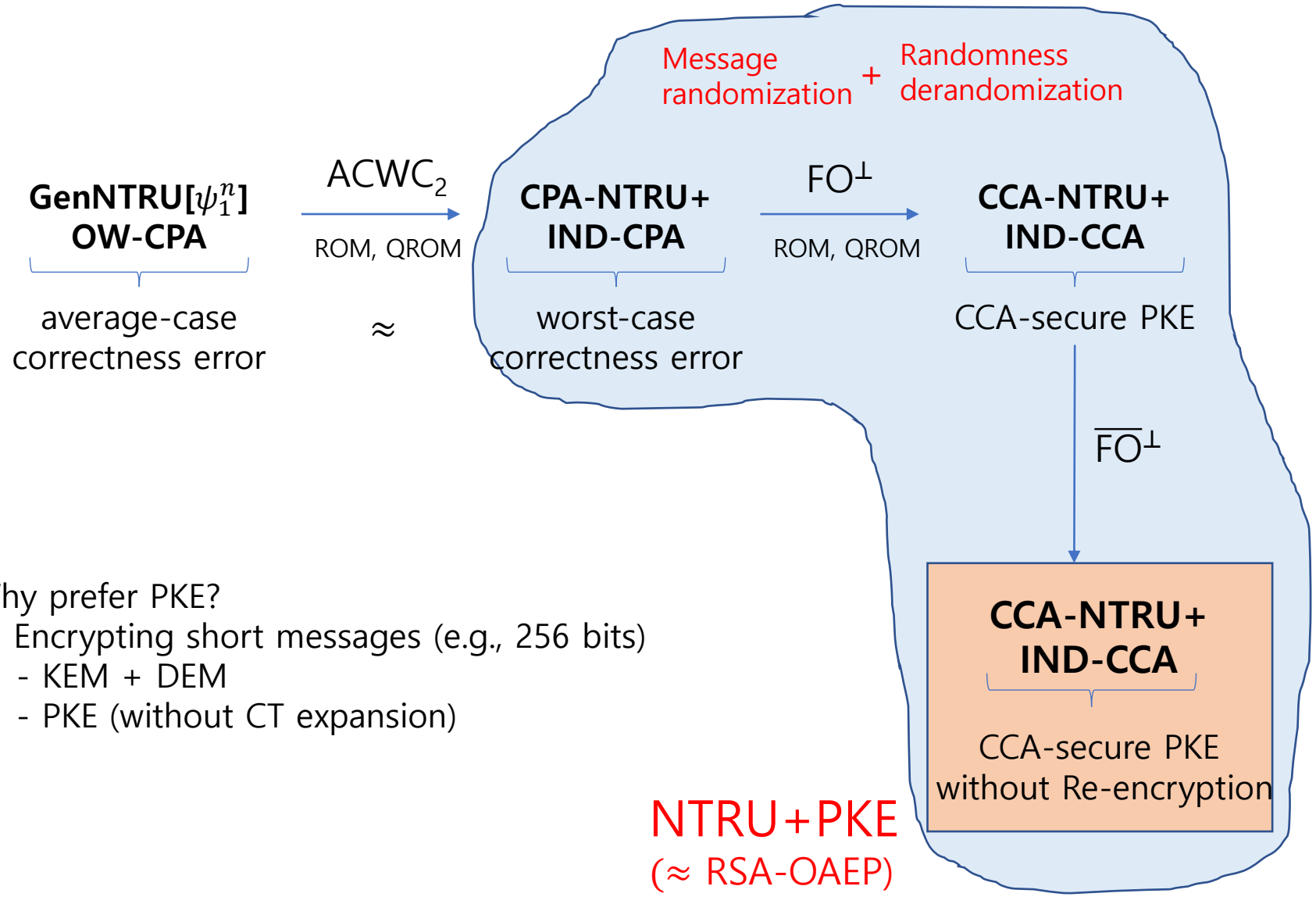
<Radix-2 NTT Layer>



<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

NTRU+ Public Key Encryption (ongoing work)



Why prefer PKE?

→ Encrypting short messages (e.g., 256 bits)

- KEM + DEM
- PKE (without CT expansion)

NTRU+PKE
(≈ RSA-OAEP)

CCA-NTRU+PKE from $\mathbf{FO}^{\perp}$

- **KeyGen**(1^{λ})
  - $(pk, sk) = \mathbf{Gen}(1^{\lambda})$
    - $\mathbf{f}', \mathbf{g} \leftarrow \boldsymbol{\psi}_1^{\boldsymbol{n}}$
    - $\mathbf{f} = 3\mathbf{f}' + 1$
    - check if $\mathbf{f}$ and $\mathbf{g}$ are invertible
    - $(pk, sk) = (\mathbf{h} = 3\mathbf{g}\mathbf{f}^{-1}, \mathbf{f})$

- **Enc**$(pk, m \in \{0,1\}^{n_1}; \mathbf{R} \leftarrow \{0,1\}^{n_2})$
  - $m' \leftarrow \mathbf{R}||m$
  - $\mathbf{r} = \mathbf{H}(m')$
  - $\mathbf{c} = \mathbf{Enc}'(pk, m'; \mathbf{r})$
    - $\mathbf{m} = \mathbf{SOTP}(m', \mathbf{G}(\mathbf{r}))$
    - $\mathbf{c} = \mathbf{Enc}(\mathbf{h}, \mathbf{m}; \mathbf{r})$

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

[FO99] Fujisaki et al. "How to Enhance the Security of Public-Key Encryption at Minimum Cost", PKC'99

CCA-NTRU+PKE from $\overline{\mathbf{FO}}^{\perp}$

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

- **Enc**$(pk, m \in \{0,1\}^{n_1}; \mathbf{R} \leftarrow \{0,1\}^{n_2})$
  - $m' \leftarrow \mathbf{R}||m$
  - $\mathbf{r} = \mathbf{H}(m')$
  - $\mathbf{c} = \mathbf{Enc}'(pk, m'; \mathbf{r})$
    - $\mathbf{m} = \mathbf{SOTP}(m', \mathbf{G}(\mathbf{r}))$
    - $\mathbf{c} = \mathbf{Enc}(\mathbf{h}, \mathbf{m}; \mathbf{r})$

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

Thank You

Q&A