NTRU+ 규격과 표준화 방안

2025.07.15

상명대학교 박종환

(Final) NTRU+ from $\overline{\mathbf{FO}}^{\perp}$

- SOTP using CBD sampling
- ACWC_2 transform
- FO without re-encryption
- Explicit rejection $\perp$

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
  - $(pk, sk) = (3\mathbf{g}\mathbf{f}^{-1}, \mathbf{f})$

Encap

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

Decap

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

FO Transform for KEM

- **FO(Fujisaki-Okamoto) transform for KEM**
  - OW/CPA-secure PKE → CCA-secure KEM

- **Requirements for underlying OW/CPA-secure PKE**
  - Worst-case correctness error
  - Message space with at least 256 min-entropy
  - Depending on whether γ-spreadness holds,
    - Two types of decapsulation algorithms exist → $\mathrm{FO}^{\perp}$, $\mathrm{FO}^{\not\perp}$

- (Statistical) γ**-spreadness**
  - For fixed message m and ciphertext c, $\Pr_{r \leftarrow \psi_{\mathcal{R}}}[c = Enc(pk, m\, ; r)] \leq 2^{-\gamma}$

FO Transform with Explicit Rejection

❖ CPA-secure PKE meets γ-spreadness (→ NTRU+)

$$\mathbf{PKE}' = (\mathbf{Gen}', \mathbf{Enc}', \mathbf{Dec}') \xrightarrow{\mathrm{FO}^{\perp}} \mathbf{KEM}'' = (\mathbf{Gen}'', \mathbf{Encap}'', \mathbf{Decap}'')$$

CPA-secure PKE

CCA-secure KEM

◆ **Encap''**(pk)

- $m \leftarrow \{0,1\}^n$
- $(K, \mathbf{r}) = \mathbf{H}(m)$
- $\boldsymbol{c} = \mathbf{Enc}'(pk, m; \mathrm{r})$
- **return** $(\boldsymbol{c}, K)$

◆ **Decap''**(sk, c)

- $m' = \mathbf{Dec}'(sk, c)$
- $(K', \mathbf{r}') = \mathbf{H}(m')$
- $\mathrm{c} = \mathbf{Enc}'(pk, m'; r')$
- If $c = c'$, return K'. Else, return $\perp$

Re-encryption

FO Transform with Implicit Rejection

❖ **CPA-secure PKE does not meet γ-spreadness (→ Kyber, SMAUG-T)**

$$\underset{\text{CPA-secure PKE}}{\boxed{\mathbf{PKE}' = (\mathbf{Gen}', \mathbf{Enc}', \mathbf{Dec}')}} \xrightarrow{\mathrm{FO}^{\not\perp}} \underset{\text{CCA-secure KEM}}{\boxed{\mathbf{KEM}'' = (\mathbf{Gen}'', \mathbf{Encap}'', \mathbf{Decap}'')}}$$

- **Encap″**(pk)
  - $m \leftarrow \{0,1\}^n$
  - $(K, \mathbf{r}) = \mathbf{H}(m)$
  - $\boldsymbol{c} = \mathbf{Enc}'(pk, m; \mathrm{r})$
  - **return** $(\boldsymbol{c}, K)$
- **Decap″**(sk, c)
  - $m' = \mathbf{Dec}'(sk, c)$
  - $(K', \mathbf{r}') = \mathbf{H}(m')$
  - $\mathrm{c} = \mathbf{Enc}'(pk, m'; r')$ — Re-encryption
  - $K'' = \mathbf{PRF}(\boldsymbol{k}, c)$
  - If $c = c'$, return K'. Else, return K''

Parameters for NTRU+

❖ 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
~~NTRU+576~~	~~1~~	~~576~~	3457	~~864~~	~~864~~	~~1,760~~	~~2^{-487}~~	~~111~~	~~99~~
NTRU+768	1+	768		1,152	1,152	2,336	2^{-379}	156	139
NTRU+864	3	864		1,296	1,296	2,624	2^{-340}	179	160
NTRU+1152	5	1152		1,728	1,728	3,488	2^{-260}	248	222

Performance Comparison - KEMs

Algorithm	sec. (c)	n	q	PK (Byte)	CT (Byte)	SK (Byte)	$\log_2\delta$	Optimized C (K Cycles)			AVX2 (K Cycles)		
								Gen	Encap	Decap	Gen	Encap	Decap
NTRU+576	111	576	3,457	864	864	1,760	-487	102	60	58	26	26	16
NTRU+768	156	768		1,152	1,152	2,336	-379	124	80	75	28	32	19
NTRU+864	179	864		1,296	1,296	2,624	-340	147	91	87	30	36	22
NTRU+1152	248	1,152		1,728	1,728	3,488	-260	226	118	119	46	47	29
Kyber512	115	256x2	3,329	800	768	1,632	-139	132	157	199	27	29	30
Kyber768	174	256x3		1,184	1,088	2,400	-164	231	256	316	45	44	46
Kyber1024	241	256x4		1,568	1,568	3,168	-174	337	387	464	62	63	67
TiMER	112	256x2	1,024	672	608	832	-161	117	102	137	42	25	35
SMAUG-T 128	112	256x2	1,024	672	672	832	-118	116	103	136	42	25	34
SMAUG-T 192	174	256x3	2,048	1,088	992	1,312	-179	222	205	254	60	47	61
SMAUG-T 256	236	256x4	2,048	1,440	1,374	1,792	-194	357	337	401	82	66	85

Test Environment: Intel Core i7-8700K @ 3.70GHz (Single Core, Hyper-Threading Disabled), 64GB RAM, Ubuntu 22.04 LTS, GCC 11.4

Lattice Estimator : https://github.com/malb/lattice-estimator/tree/5ba00f56dd1086c3a42b98fc596c64907adb96ff

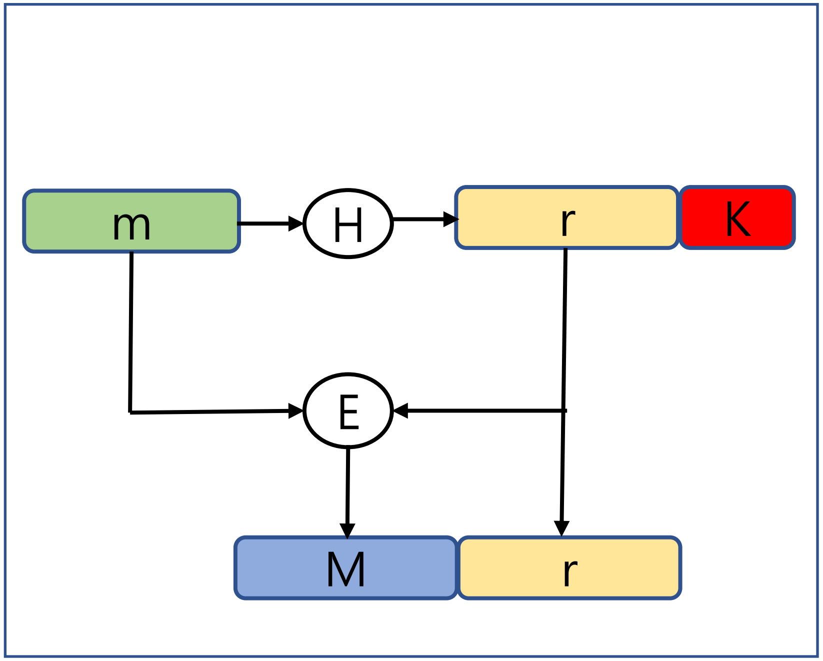
Kyber source code : https://github.com/pq-crystals/kyber/tree/4768bd37c02f9c40a46cb49d4d1f4d5e612bb882

SMAUG-T source code : https://github.com/hmchoe0528/SMAUG-T_public/tree/1f451c2232cd4e5afd408f2ebacbddb98daef200

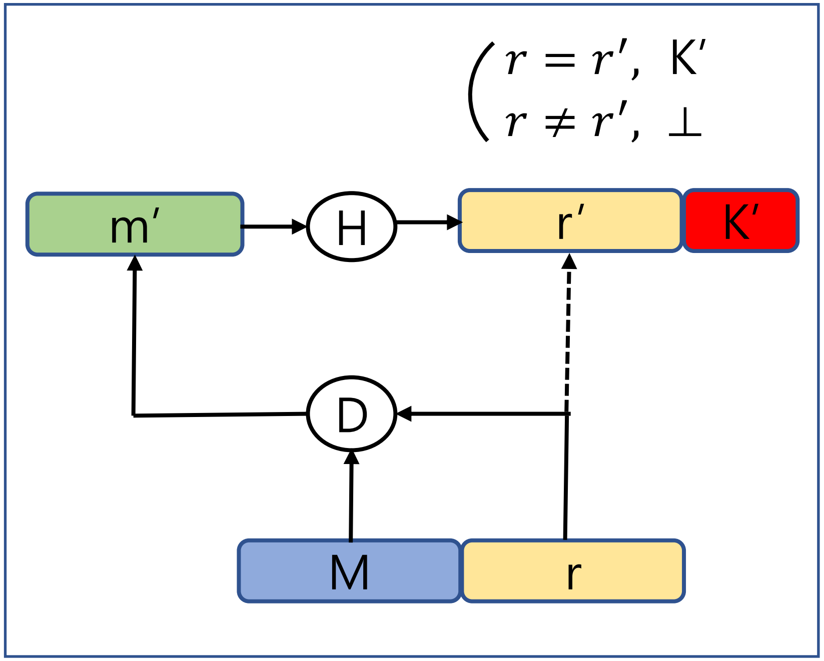
❖ OAEP(Optimal Asymmetric Encryption Padding) for KEM

- Using the fact that NTRU+ is deterministic PKE

<OAEP encoding>



<OAEP decoding>



- H: hash function
- SOTP = (E, D)

CCA Attack + Side-Channel Info. against Kyber

❖ **Using decap. Oracles + side-channel analysis**

c →

← K

◆ **Decap''**(sk, c)

- $m' = \mathbf{Dec}'(sk, c)$
- $(K', \mathbf{r}') = \mathbf{H}(m')$
- $\mathrm{c} = \mathbf{Enc}'(pk, m'; r')$
- $K'' = \mathbf{PRF}(\boldsymbol{k}, c)$
- If $c = c'$, return K'. Else, return K''

Side-channel info.

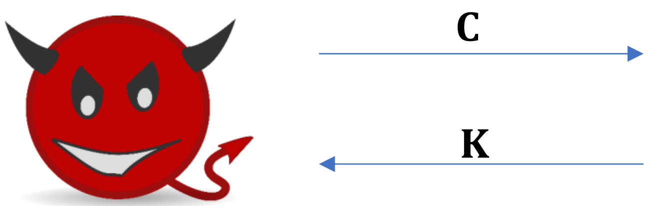
❖ **In chosen-ciphertext attacks on C=Encap''(pk, m)**

- Side-channel info. = same m ??? → private key(sk) recovery !

[UXT+22] Ueno et al., "Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs," TCHES 2022.

CCA Attack + Side-Channel Info. against NTRU+

❖ **Using decap. Oracles + side-channel analysis**



◆ **Decap″**(sk, c)

- $\mathbf{m}' = \mathbf{Dec}'(sk, \mathbf{c})$
  - $\mathbf{m}' = \mathbf{Dec}(\mathbf{f}, \mathbf{c})$
  - $\mathbf{r}' = \mathbf{RRec}(\mathbf{h}, \mathbf{c}, \mathbf{m}')$
  - $m' = \mathbf{Inv}\big(\mathbf{m}', \mathbf{G}(\mathbf{r}')\big)$
- $(K', \mathbf{r}'') = \mathbf{H}(m')$
- If $\mathbf{r}' == \mathbf{r}''$
  - Return K', else return $\perp$

Side-channel info.

❖ **In chosen-ciphertext attacks on C=Encap″(pk, m)**

- Side-channel info. = same $\mathbf{r}$??? → message(m) recovery !

❖ **Rabin(sk recovery) vs. RSA(m recovery)**

Comparison to Kyber and SMAUG-T

Scheme	SMAUG-T [CCH+23]	Kyber [BDK+18]	NTRU+[KP23]
NTT-friendly	No	Yes	Yes
Correctness error	Worst-case	Worst-case	Worst-case
Message set	$m \leftarrow \{0,1\}^{256}$	$m \leftarrow \{0,1\}^{256}$	$m \leftarrow \{0,1\}^{n}$
Message distribution	Uniform	Uniform	Arbitrary
CCA transform	$\mathrm{FO}^{\not\perp}$	$\mathrm{FO}^{\not\perp}$	$\mathrm{ACWC}_2 + \overline{\mathrm{FO}}^{\perp}$
Hardness assumptions	Module RLWE	Module RLWE	NTRU, RLWE
Re-encryption in Decap.	Yes	Yes	No
In response to invalid CT	PRF key	PRF key	$\perp$
CCA attack + SCA	Private key recovery	Private key recovery	Message recovery

[CCH+23] Cheon et al. "SMAUG: Pushing Lattice-Based Key Encapsulation Mechanisms to the Limits", SAC 2023
[BDK+18] Bos et al. "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM", IEEE EuroS&P 2018
[KP23] Kim et al. "NTRU+: Compact Construction of NTRU Using Simple Encoding Method", IEEE TIFS, 18 (2023)

KS 표준 문서 추진 계획

❖ KS 표준 문서 작성 일정

	6월	7월	8월	9월	10월	11월
선행 표준화 사례 조사						
표준 구성 및 작성 계획 수립						
초안 완성						
최종안 완성						

❖ KS 표준 문서 작성시 고려사항

- 개념의 명확성을 고려한 용어 및 명칭 사용
- 국제 표준을 목표로 ISO 등 국제 표준 문서를 참고하여 작성
- 기존 국제 표준을 참조하여 기법 내의 함수 구성을 정의
- 비전문가가 이해할 수 있도록 각 세부 알고리즘을 함수로 표현

Thank You

Q&A