Improvements in NTRU+

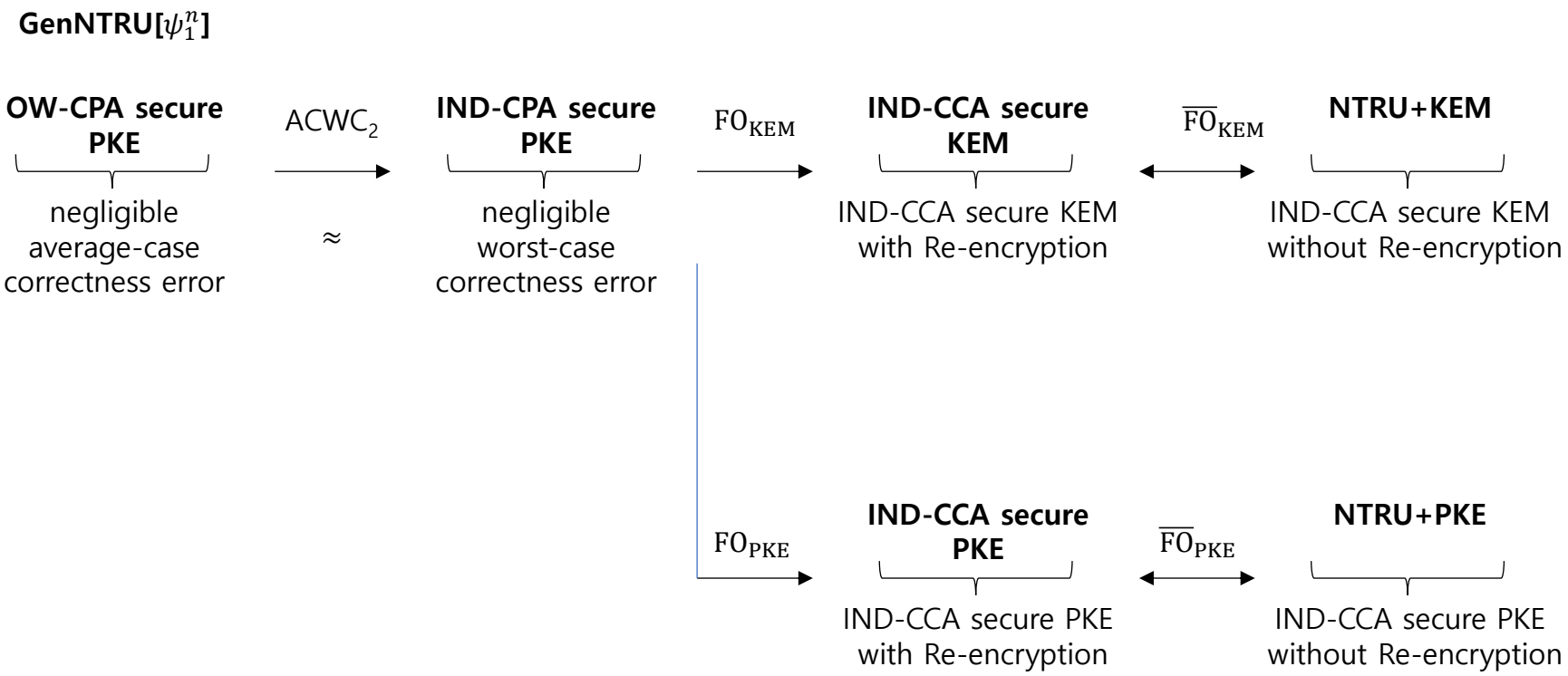
2024.10.22.

Korea University

Jonghyun Kim

NTRU+

❖ NTRU-based IND-CCA secure KEM & PKE



Changes in NTRU+ Version 2.2 & 2.2.1

❖ Goal

- Improve the efficiency of the key generation algorithm !

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+KEM 576	114	576	3,457	864	864	1,760	-487	274 ↓ 167	102 ↓ 80	128 ↓ 95	21 ↓ 24	23 ↓ 22	14 ↓ 13
NTRU+KEM 768	164	768		1,152	1,152	2,336	-379	325 ↓ 192	133 ↓ 101	172 ↓ 121	26 ↓ 26	30 ↓ 27	19 ↓ 16
NTRU+KEM 864	189	864		1,296	1,296	2,624	-340	314 ↓ 238	157 ↓ 123	207 ↓ 148	24 ↓ 28	32 ↓ 30	21 ↓ 19
NTRU+KEM 1152	263	1,152		1,728	1,728	3,488	-260	751 ↓ 370	198 ↓ 162	274 ↓ 196	45 ↓ 41	39 ↓ 39	25 ↓ 26

Changes in NTRU+ Version 2.2 & 2.2.1

❖ Changes in the Specification & Implementation

◆ 1. Hash function

- Replaced AES256CTR with SHAKE256 for hash function instantiation

◆ 2. Key generation algorithm

- Samples the polynomials f and g separately
- Uses early abort in the invertibility test

◆ 3. Ring operation

- Modified the NTT structures for NTRU+{KEM, PKE}{576, 768, 1152}
- Applied the Montgomery reduction lazily
- Improved the modulus inversion

Key Generation Algorithm

❖ **Samples the polynomials f and g separately**

Algorithm 15 Gen(1^λ): key generation

Ensure: Public key $pk \in \mathcal{B}^{\lceil \log_2 q \rceil \cdot n/8}$
Ensure: Secret key $sk \in \mathcal{B}^{\lceil \log_2 q \rceil \cdot n/4}$
1: $d \leftarrow \mathcal{B}^{32}$
2: $(f, g) := \mathsf{XOF}(d, n/2)$
3: $\mathbf{f}' := \mathsf{CBD}_1(f)$, $\mathbf{g}' := \mathsf{CBD}_1(g)$
4: $\mathbf{f} = 3\mathbf{f}' + 1$
5: $\mathbf{g} = 3\mathbf{g}'$
6: $\hat{\mathbf{f}} = \mathsf{NTT}(\mathbf{f})$, $\hat{\mathbf{g}} = \mathsf{NTT}(\mathbf{g})$
7: **if** $\mathbf{f}$ or $\mathbf{g}$ is not invertible in R_q, restart
8: $\hat{\mathbf{h}} = \hat{\mathbf{g}} \circ \hat{\mathbf{f}}^{-1}$
9: $pk := \mathsf{Encode}_q(2^{16} \cdot \hat{\mathbf{h}})$
10: $sk := \mathsf{Encode}_q(\hat{\mathbf{f}}) || \mathsf{Encode}_q(2^{16} \cdot \hat{\mathbf{h}}^{-1}) || \mathsf{F}(pk)$
11: **return** (pk, sk)

Version 2.0

Algorithm 15: Gen(1^λ): key generation

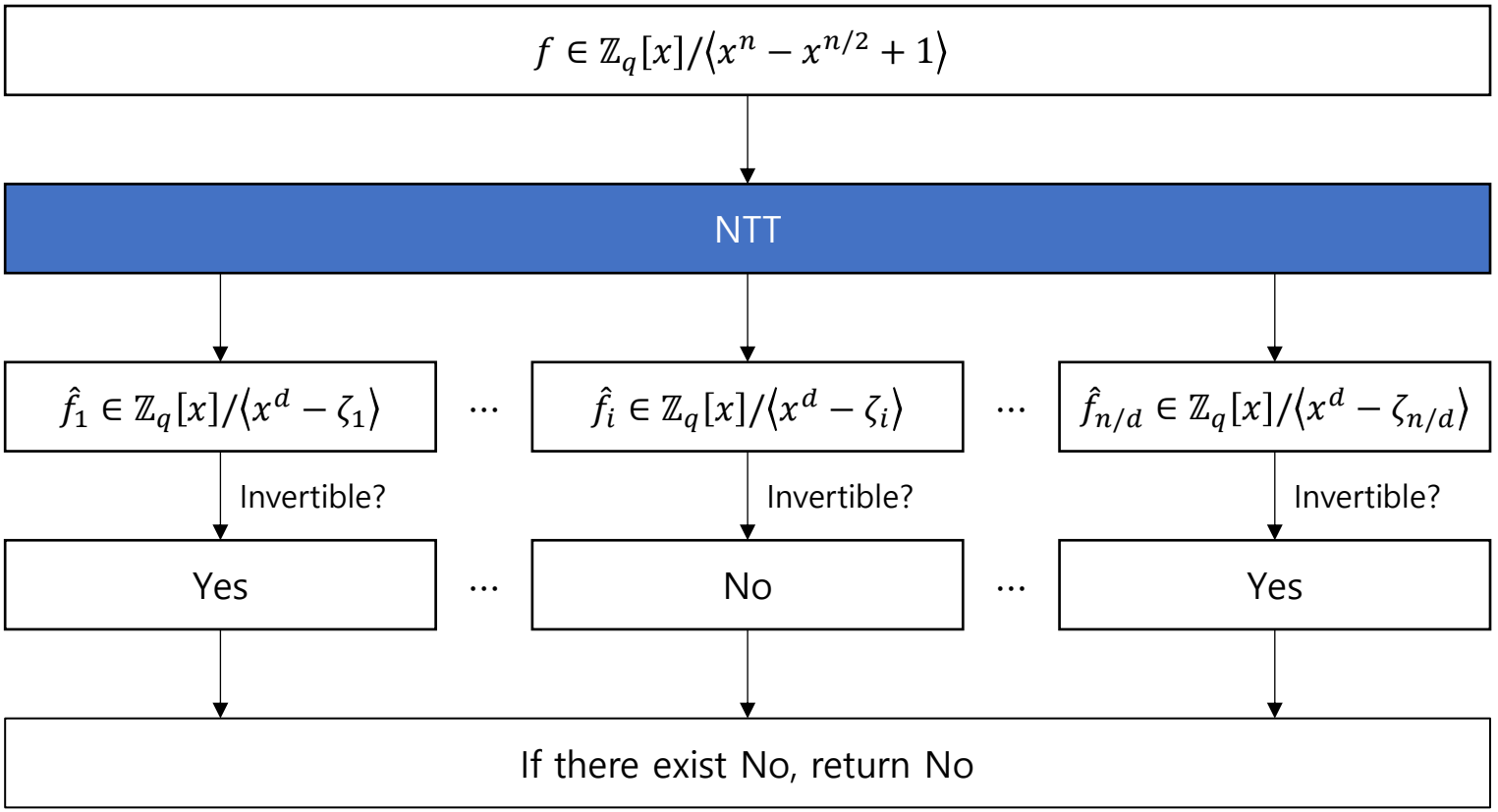
Ensure: Public key $pk \in \mathcal{B}^{\lceil \log_2 q \rceil \cdot n/8}$
Ensure: Secret key $sk \in \mathcal{B}^{\lceil \log_2 q \rceil \cdot n/4}$
1: **repeat**
2: $d \leftarrow \mathcal{B}^{32}$
3: $f := \mathsf{XOF}(d, n/4)$
4: $\mathbf{f}' := \mathsf{CBD}_1(f)$
5: $\mathbf{f} := 3\mathbf{f}' + 1$
6: $\hat{\mathbf{f}} := \mathsf{NTT}(\mathbf{f})$
7: **until** $\mathbf{f}$ is invertible in R_q
8: **repeat**
9: $d \leftarrow \mathcal{B}^{32}$
10: $g := \mathsf{XOF}(d, n/4)$
11: $\mathbf{g}' := \mathsf{CBD}_1(g)$
12: $\mathbf{g} := 3\mathbf{g}'$
13: $\hat{\mathbf{g}} := \mathsf{NTT}(\mathbf{g})$
14: **until** $\mathbf{g}$ is invertible in R_q
15: $\hat{\mathbf{h}} := \hat{\mathbf{g}} \circ \hat{\mathbf{f}}^{-1}$
16: $pk := \mathsf{Encode}_q(2^{16} \cdot \hat{\mathbf{h}})$
17: $sk := \mathsf{Encode}_q(\hat{\mathbf{f}}) || \mathsf{Encode}_q(2^{16} \cdot \hat{\mathbf{h}}^{-1}) || \mathsf{F}(pk)$
18: **return** (pk, sk)

Version 2.2

Key Generation Algorithm

❖ Uses early abort in the invertibility test

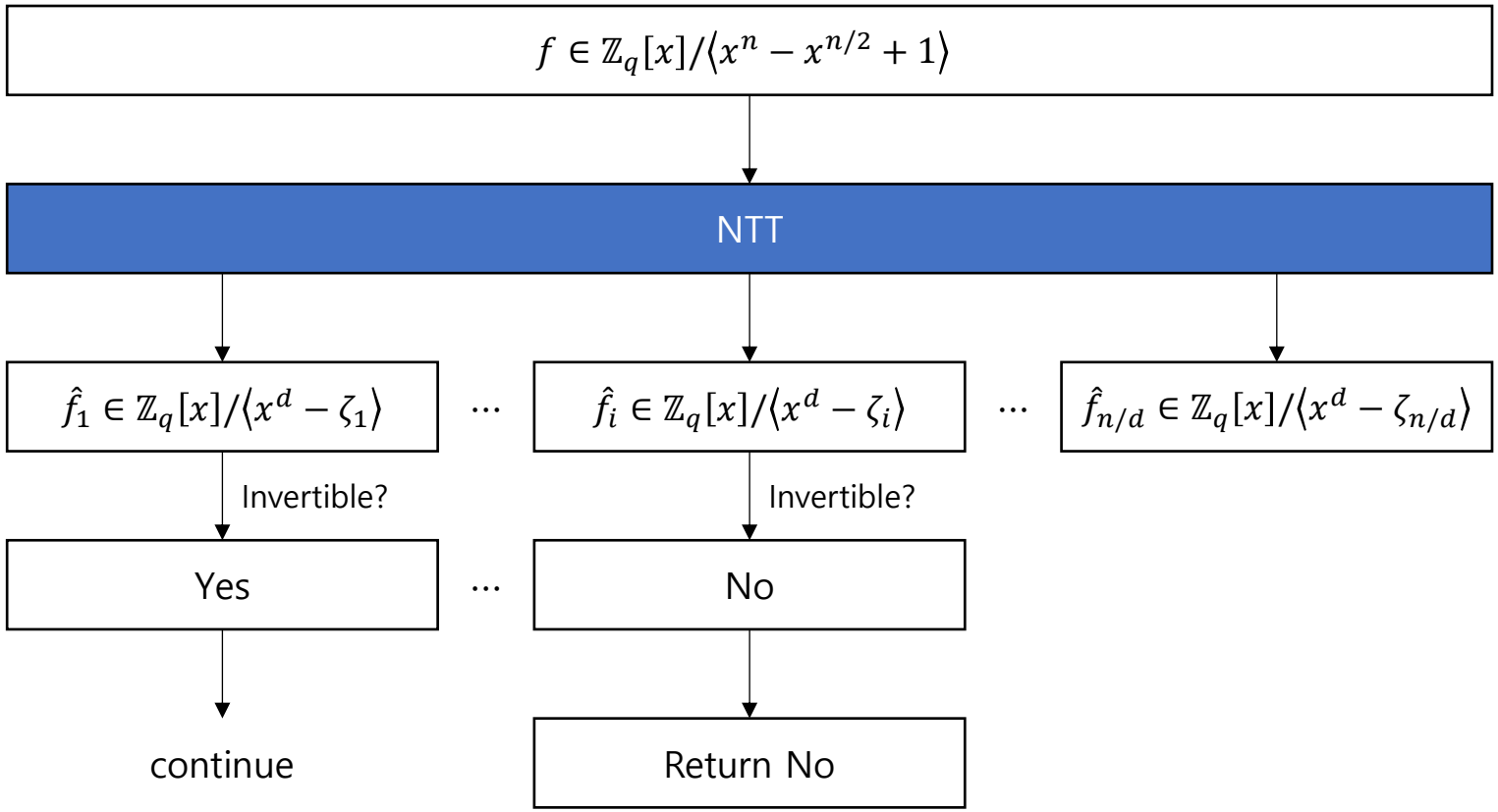
- Invertibility Test



Key Generation Algorithm

❖ Uses early abort in the invertibility test

- Invertibility Test with Early Abort



Ring Operation

❖ Modified the NTT structures for NTRU+{KEM, PKE}{576, 768, 1152}

- NTT structure for $\mathbb{Z}_{3457}[x]/\langle x^n - x^{n/2} + 1\rangle$ with $n = 576$
  - Similar analysis can be applied to $n = 768, 1152$

	Naïve	Version 1.0	Version 1.1	Version 2.2
Radix-2 NTT layers	6	5	6	4
Radix-3 NTT layers	2	2	1	2
Result of NTT	$\prod_{i=1}^{576}\mathbb{Z}_{3457}[x]/\langle x-\psi_i\rangle$	$\prod_{i=1}^{288}\mathbb{Z}_{3457}[x]/\langle x^2-\eta_i\rangle$	$\prod_{i=1}^{192}\mathbb{Z}_{3457}[x]/\langle x^3-\xi_i\rangle$	$\prod_{i=1}^{144}\mathbb{Z}_{3457}[x]/\langle x^4-\xi_i\rangle$
Polynomial inversion	576 modulus inversions	288 modulus inversions	192 modulus inversions	144 modulus inversions
Precomputation table	576 elements	288 elements	192 elements	144 elements

- The ideas from **[ZFY23]** were adapted to implement efficient inversion in $\mathbb{Z}_{3457}[x]/\langle x^4 - \xi_i\rangle$.
  - It computes the inversion in $\mathbb{Z}_{3457}[x]/\langle x^n - \xi_i\rangle$ by using the inversion in $\mathbb{Z}_{3457}[x]/\langle x^{n/2} - \xi_i\rangle$

[ZFY23] Zhang et. al., "Faster and Smaller NTRU Encryption using Vector Decoding", ASIACRYPT 2023

Ring Operation

❖ Applied the Montgomery reduction lazily

- Multiplication in $R_q = \mathbb{Z}_q[x]/\langle x^3 - \zeta \rangle$
  - $a(x) = a_0 + a_1 x + a_2 x^2 \in R_q$
  - $b(x) = b_0 + b_1 x + b_2 x^2 \in R_q$
  - $c(x) = a(x)b(x)$
    - $c_0 = a_0 b_0 + (a_1 b_2 + a_2 b_1)\zeta$
    - $c_1 = a_0 b_1 + a_1 b_0 + a_2 b_2 \zeta$
    - $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$
- Multiplication with Montgomery & Barrett reduction

$$a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$barrett\big(mont(a_0 \cdot b_2) + mont(a_1 \cdot b_1) + mont(a_2 \cdot b_0)\big) \quad \Rightarrow \quad mont(a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0)$$

Apply Montgomery reduction lazily

This technique is already applied in NCC-Sign Version 2.1

Ring Operation

❖ Improved the modulus inversion

◆ Modulus inversion

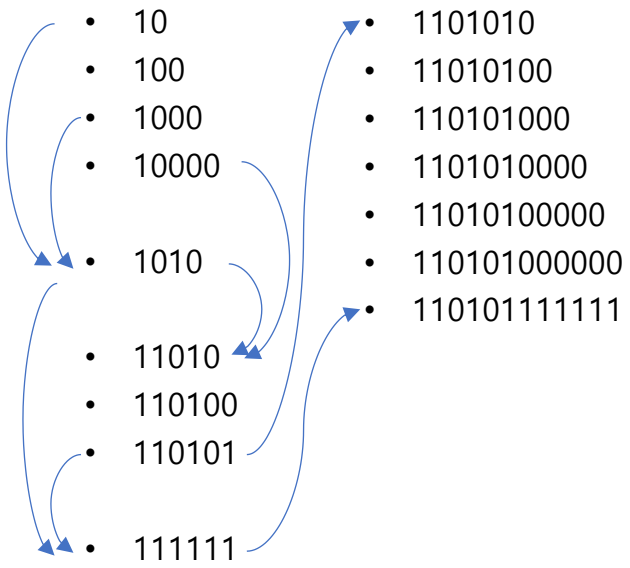
- $a^{-1} \equiv a^{q-2} \pmod{q}$, $q - 2 = 3455 = 110101111111_{(2)}$

- Modulus inversion with Square-and-Multiply

  - 10
  - 11
  - 110
  - 1100
  - 1101
  - 11010
  - 110100
  - 110101
  - 1101010
  - 1101011
  - 11010110
  - 11010111
  - 110101110
  - 110101111
  - 1101011110
  - 1101011111
  - 11010111110
  - 11010111111
  - 110101111110
  - 110101111111

20 multiplications

- Improved Modulus inversion



16 multiplications

Performance Comparison

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+KEM 576	114	576	3,457	864	864	1,760	-487	167	80	95	24	22	13
NTRU+KEM 768	164	768		1,152	1,152	2,336	-379	192	101	121	26	27	16
NTRU+KEM 864	189	864		1,296	1,296	2,624	-340	238	123	148	28	30	19
NTRU+KEM 1152	263	1,152		1,728	1,728	3,488	-260	370	162	196	41	39	26
Kyber512	117	256x2	3,329	800	768	1,632	-139	116	137	158	36	39	24
Kyber768	181	256x3		1,184	1,088	2,400	-164	182	202	230	51	55	37
Kyber1024	253	256x4		1,568	1,568	3,168	-174	270	321	359	65	73	52
NTRUHPS 2048509	106	509	2,048	699	699	935	-∞	8,031	746	1,384	376	262	33
NTRUHRSS 701	136	701	8,192	1,138	1,138	1,450	-∞	14,684	1030	2,623	365	166	52
NTRUHPS 2048677	145	677	2,048	930	930	1,234	-∞	13,882	1206	2,441	545	348	49
NTRUHPS 4096821	179	821	4096	1,230	1,230	1,590	-∞	20,385	1,644	3,519	702	423	62

Thank You

Q&A