NTRU+

Compact Construction of NTRU Using Simple Encoding Method

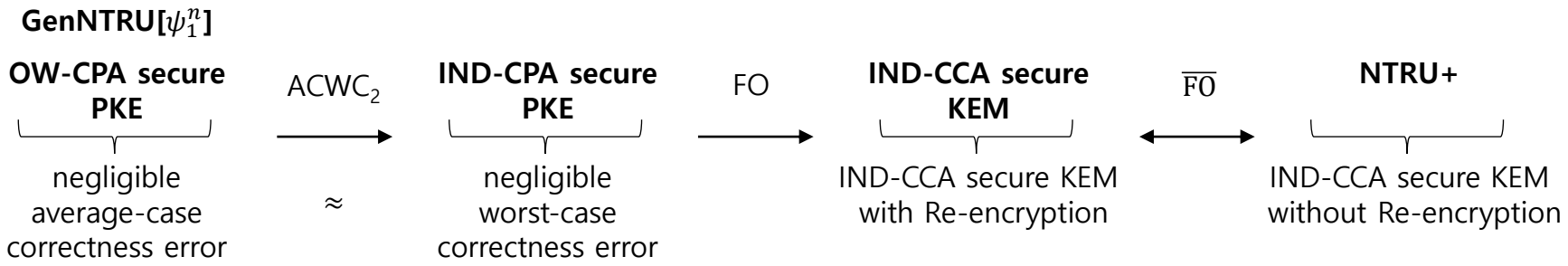
2023.11.13.

고려대학교

김 종 현

Overview of NTRU+

❖ Overview



Changes in NTRU+

❖ NTRU+ Specification Version 1.1

- can be found at https://sites.google.com/view/ntruplus/resources

❖ Changes in Specification Version 1.1

- 1. Countermeasure against Multi-target Attack
- 2. Countermeasure against CCA Attack of **[LLP23]**
- 3. Modified NTT structures for NTRU+576 & NTRU+1152
  - Enhanced the speed of key generation algorithm
  - Reduced the size of precomputation tables

[LLP23] Lee et al. "A Novel CCA Attack for NTRU+ KEM", EPRINT 2023

Countermeasure against Multi-target Attack

❖ NTRU+

◆ Gen(1^λ)

- Run until both $\mathbf{f}$ and $\mathbf{g}$ are invertible
  - $\mathbf{f}', \mathbf{g} \leftarrow \psi_1^n$
  - $\mathbf{f} = 3\mathbf{f}' + 1$
- $pk = \left(\mathbf{h} = 3\mathbf{g}\mathbf{f}^{-1}\right)$
- $sk = \left(\mathbf{f}, \mathbf{h}^{-1}, \mathbf{F}(pk)\right)$ ➔ sk size ↑ by 32bytes

◆ Encap(pk)

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

◆ Decap$(sk, \mathbf{c})$

- $\mathbf{m}' = \mathbf{Dec}(\mathbf{f}, \mathbf{c})$
- $\mathbf{r}' = \mathbf{h}^{-1}(\mathbf{c} - \mathbf{m}')$
- $m' = \mathbf{Inv}\left(\mathbf{m}', \mathbf{G}(\mathbf{r}')\right)$
- $(K', \mathbf{r}'') = \mathbf{H}\left(m', \mathbf{F}(pk)\right)$
- If $\mathbf{r}' == \mathbf{r}''$, Return K'
- Else, return $\perp$

Countermeasure against CCA Attack of [LLP23]

❖ [LLP23] CCA against NTRU+

- $\mathbf{m} = \mathbf{SOTP}\big(m, \mathbf{G}(\mathbf{r}) = (u_1, u_2)\big)$
  - $\mathbf{m} = (m \oplus u_1) - u_2$
- $m' = \mathbf{Inv}\big(\mathbf{m}, u = (u_1, u_2)\big)$
  - $m' = (\mathbf{m} + u_2) \oplus u_1$
  - $m' = \big((\mathbf{m} + u_2) \bmod 2\big) \oplus u_1$

- $\mathbf{Inv}(\mathbf{m}, u = (u_1, u_2))$
  - $t = \mathbf{m} + u_2$
  - If $t \notin \{0,1\}^n$, **return** $\perp$.
  - Else, $m' = t \oplus u_1$
  - **return** $m' \in \{0,1\}^n$

- $\mathbf{c} = \mathbf{hr} + \mathbf{m}$
  - $u = (u_1, u_2) = \mathbf{G}(\mathbf{r})$
  - $\mathbf{m} = \mathbf{SOTP}(m, u)$
  - $[\mathbf{m}]_1 = -1, [u_2]_1 = 1$ ➔ $[\mathbf{m}]_1 + [u_2]_1 = 0$

Same value

- $\mathbf{c}' = \mathbf{c} + (2,0,\cdots,0) = \mathbf{hr} + \mathbf{m} + (2,0,\cdots,0)$
  - $\mathbf{m}' = \mathbf{SOTP}(m, u) + (2,0,\cdots,0)$
  - $[\mathbf{m}']_1 = 1, [u_2]_1 = 1$ ➔ $[\mathbf{m}']_1 + [u_2]_1 \equiv 0 \pmod 2$

➔ Recover same m'

➔ Compute same $(K', \mathbf{r}'') = \mathbf{H}(m')$

➔ Pass validity check $\mathbf{r}' == \mathbf{r}''$

➔ $\mathbf{Decap}(sk, \mathbf{c}) = \mathbf{Decap}(sk, \mathbf{c}') = K'$

< CCA against NTRU+ >

[LLP23] Lee et al. "A Novel CCA Attack for NTRU+ KEM", EPRINT 2023

NTT for $\mathbb{Z}_{3457}[x]/\langle x^{576}-x^{288}+1\rangle$

❖ NTT Layers

- Radix-2 NTT layer
  - $\mathbb{Z}_q[x]/\langle x^n-\psi^2\rangle \approx \mathbb{Z}_q[x]/\langle x^{n/2}-\psi\rangle \times \mathbb{Z}_q[x]/\langle x^{n/2}+\psi\rangle$
  - $\mathbb{Z}_q[x]/\langle x^n-x^{n/2}+1\rangle \approx \mathbb{Z}_q[x]/\langle x^{n/2}-\zeta\rangle \times \mathbb{Z}_q[x]/\langle x^{n/2}-\zeta^5\rangle$
    - ζ: primitive 6th root of unity modulo q
- Radix-3 NTT layer
  - $\mathbb{Z}_q[x]/\langle x^n-\alpha^3\rangle \approx \mathbb{Z}_q[x]/\langle x^{n/3}-\alpha\rangle \times \mathbb{Z}_q[x]/\langle x^{n/3}-\alpha\omega\rangle \times \mathbb{Z}_q[x]/\langle x^{n/3}-\alpha\omega^2\rangle$
    - ω : primitive 3rd root of unity modulo q

❖ NTT for $\mathbb{Z}_{3457}[x]/\langle x^{576}-x^{288}+1\rangle$

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

- Similar analysis can be applied to $\mathbb{Z}_{3457}[x]/\langle x^{1152}-x^{576}+1\rangle$

Changes in NTRU+

❖ Changes in Implementation (https://github.com/ntruplus/ntruplus)

- 1. Removed the dependencies on OpenSSL and AVX in ref. Implementation

- 2. Modified Radix-3 NTT Implementation based on **[HY22]**
  - Reduced number of required multiplications from $4n/3$ to n

$$\hat{a}_0(x) = a_0(x) + a_1(x)\alpha + a_2(x)\alpha^2$$
$$\hat{a}_1(x) = a_0(x) - a_2(x)\alpha^2 + \omega(a_1(x)\alpha - a_2(x)\alpha^2)$$
$$\hat{a}_2(x) = a_0(x) - a_1(x)\alpha - \omega(a_1(x)\alpha - a_2(x)\alpha^2)$$

- 3. Reduced the pre-computation table size in the ref. implementation
  - Removed the precomputation tables for the InvNTT

$$3a_0(x) = \hat{a}_0(x) + \hat{a}_1(x) + \hat{a}_2(x)$$
$$3a_1(x) = (w\alpha^{-1})(\hat{a}_2(x) - \hat{a}_0(x) + (\hat{a}_1(x) - \hat{a}_0(x))w)$$
$$3a_2(x) = (w^2\alpha^{-2})(\hat{a}_2(x) - \hat{a}_1(x) - (\hat{a}_1(x) - \hat{a}_0(x))w)$$

Instead of using values from precomputation table for InvNTT, we reuse values from precomputation table for NTT

[HY22] Hassan et al. "Radix-3 NTT-Based Polynomial Multiplication for Lattice-Based Cryptography", EPRINT 2022

Performance Comparison

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~~ 1,760	-487	~~321~~ 285	~~111~~ 106	~~163~~ 135	~~17~~ 20	~~14~~ 20	12
NTRU+ 768	161	768		1,152	1,152	~~2,304~~ 2,336	-379	~~314~~ 325	~~146~~ 137	~~227~~ 177	~~16~~ 24	~~18~~ 26	~~16~~ 17
NTRU+ 864	188	864		1,296	1,296	~~2,592~~ 2,624	-340	~~340~~ 324	~~170~~ 162	~~262~~ 217	~~14~~ 23	~~19~~ 28	18
NTRU+ 1152	264	1,152		1,728	1,728	~~3,456~~ 3,488	-260	~~905~~ 770	~~230~~ 204	~~348~~ 288	~~43~~ 45	~~26~~ 36	24
Kyber 512	117	256x2	3,329	800	768	1,632	-139	103	129	156	27	35	26
Kyber 768	181	256x3		1,184	1,088	2,400	-164	184	217	253	43	55	42
Kyber 1024	253	256x4		1,568	1,568	3,168	-174	283	317	362	61	80	64
NTRUHPS 2048509	106	509	2,048	699	699	935	-∞	8,428	596	1,435	195	84	33
NTRUHRSS 701	136	701	8,192	1,138	1,138	1,450	-∞	15,603	938	2,655	257	60	51
NTRUHPS 2048677	145	677	2,048	930	930	1,234	-∞	14,461	993	2,478	307	114	49
NTRUHPS 4096821	179	821	4096	1,230	1,230	1,590	-∞	21,403	1,401	3,597	417	136	62

Thank You

Q&A