Compact and Simple RLWE Based Key Encapsulation Mechanism

Erdem Alkım[1] **Yusuf Alper Bilgin**[2,3] Murat Cenk[3]

[1] Department of Computer Engineering, Ondokuz Mayıs University, Turkey

[2] Aselsan Inc., Turkey

[3] Institude of Applied Mathematics, Middle East Technical University, Turkey

y.alperbilgin@gmail.com

October 3, 2019

aselsan

Overview

NIST PQC Standardization Project

The ~~1st Round~~ 2nd Round Candidates

	Signatures		KEM/Encryption		Overall	
Lattice-based	~~5~~	3	~~21~~	9	~~26~~	12
Code-based	~~2~~	0	~~17~~	7	~~19~~	7
Multi-variate	~~7~~	4	~~2~~	0	~~9~~	4
Symmetric-based	~~3~~	2			~~3~~	2
Other	~~2~~	0	~~5~~	1	~~7~~	1
Total	~~**19**~~	**9**	~~**45**~~	**17**	~~**64**~~	**26**

Moody, PQC Workshop, 2019

RLWE based KEM - NewHope

KEM.Setup() : $\mathbf{a} \xleftarrow{\$} \mathcal{R}_q$		
Alice		Bob
KEM.Gen($\mathbf{a}$) :		KEM.Encaps($\mathbf{a}, \mathbf{b}$) :
$\mathbf{s}, \mathbf{e} \xleftarrow{\$} \chi$		$\mathbf{s}', \mathbf{e}', \mathbf{e}'' \xleftarrow{\$} \chi$
$\mathbf{b} \leftarrow \mathbf{as} + \mathbf{e}$	$\xrightarrow{\mathbf{b}}$	$\mathbf{u} \leftarrow \mathbf{as}' + \mathbf{e}'$
		$\mathbf{v} \leftarrow \mathbf{bs}' + \mathbf{e}''$
		$\nu \xleftarrow{\$} \{0, 1\}^n$
		$\mathbf{k} \leftarrow \mathsf{Encode}(\nu)$
KEM.Decaps($\mathbf{s}, (\mathbf{u}, \mathbf{c})$) :	$\xleftarrow{\mathbf{u},\mathbf{c}}$	$\mathbf{c} \leftarrow \mathbf{v} + \mathbf{k}$
$\mathbf{v}' \leftarrow \mathbf{us}$		$\mu \leftarrow \mathsf{Extract}(\mathbf{k})$
$\mathbf{k}' \leftarrow \mathbf{c} - \mathbf{v}'$		
$\mu \leftarrow \mathsf{Extract}(\mathbf{k}')$		

Alkim et al., ePrint 2016/1157

Multiplication Algorithms

Fast multiplication algorithms: NTT, Karatsuba and Tom-Cook

Multiplication Algorithms

Fast multiplication algorithms: NTT, Karatsuba and Tom-Cook

Advantages of NTT:

- High performance

Multiplication Algorithms

Fast multiplication algorithms: NTT, Karatsuba and Tom-Cook

Advantages of NTT:

- High performance
- Memory efficient

Fast multiplication algorithms: NTT, Karatsuba and Tom-Cook

Advantages of NTT:

- High performance
- Memory efficient
- Randoms directly sampled in NTT domain

Multiplication Algorithms

Fast multiplication algorithms: NTT, Karatsuba and Tom-Cook

Advantages of NTT:

- High performance
- Memory efficient
- Randoms directly sampled in NTT domain

Disadvantages:

- Limited parametrization

NewHope-Compact

- A smaller and faster instantiation of NewHope

- A smaller and faster instantiation of NewHope
- Utilizing recent advances on NTT

- A smaller and faster instantiation of NewHope
- Utilizing recent advances on NTT
- Reduce parameter q (12289 $\rightarrow$ 3329)

NewHope-Compact

- A smaller and faster instantiation of NewHope
- Utilizing recent advances on NTT
- Reduce parameter q (12289 $\rightarrow$ 3329)
- Hybrid polynomial multiplication (NTT + Karatsuba)

NewHope-Compact

- A smaller and faster instantiation of NewHope
- Utilizing recent advances on NTT
- Reduce parameter q (12289 $\rightarrow$ 3329)
- Hybrid polynomial multiplication (NTT + Karatsuba)
- Achieving a security level equivalent to Kyber768

Number Theoretic Transform

$a \in \mathbb{Z}_q[X]/(X^n + 1)$

$$\mathrm{NTT}(a) = \hat{a} = \sum_{i=0}^{n-1} \hat{a}_i X^i, \text{ where } \hat{a}_i = \sum_{j=0}^{n-1} a_j \omega^{ij} \mod q$$

$$\mathrm{NTT}^{-1}(\hat{a}) = a = \sum_{i=0}^{n-1} a_i X^i, \text{ where } a_i = \left(n^{-1} \sum_{j=0}^{n-1} \hat{a}_j \omega^{-ij}\right) \mod q$$

$$\text{where } \omega^n = 1 \mod q$$

Number Theoretic Transform

$a \in \mathbb{Z}_q[X]/(X^n + 1)$

$$\mathrm{NTT}(a) = \hat{a} = \sum_{i=0}^{n-1} \hat{a}_i X^i, \text{ where } \hat{a}_i = \sum_{j=0}^{n-1} a_j \omega^{ij} \mod q$$

$$\mathrm{NTT}^{-1}(\hat{a}) = a = \sum_{i=0}^{n-1} a_i X^i, \text{ where } a_i = \left(n^{-1} \sum_{j=0}^{n-1} \hat{a}_j \omega^{-ij}\right) \mod q$$

$$\text{where } \omega^n = 1 \mod q$$

Polynomial Multiplication

$$c = \mathrm{NTT}^{-1}(\mathrm{NTT}(a) \circ \mathrm{NTT}(b))$$

where $a, b, c \in \mathcal{R}_q$

Butterflies

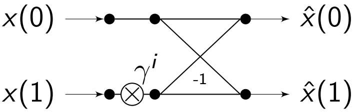


Figure: Cooley-Tukey Butterfly

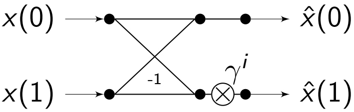


Figure: Gentleman-Sande Butterfly

CRT Map of NewHope512

Let $\gamma^{512} = -1 \mod 12289$.

$$\mathbb{Z}_{12289}/(x^{512}+1) \cong \mathbb{Z}_{12289}/(x-\gamma) \times \cdots \times \mathbb{Z}_{12289}/(x-\gamma^{511})$$

CRT Map of NewHope512

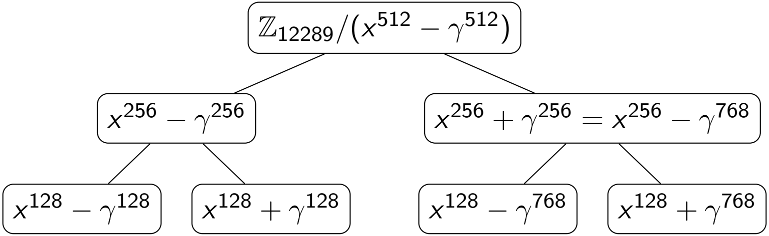
Let $\gamma^{512} = -1 \mod 12289$.

$$\mathbb{Z}_{12289}/(x^{512}+1) \cong \mathbb{Z}_{12289}/(x-\gamma) \times \cdots \times \mathbb{Z}_{12289}/(x-\gamma^{511})$$

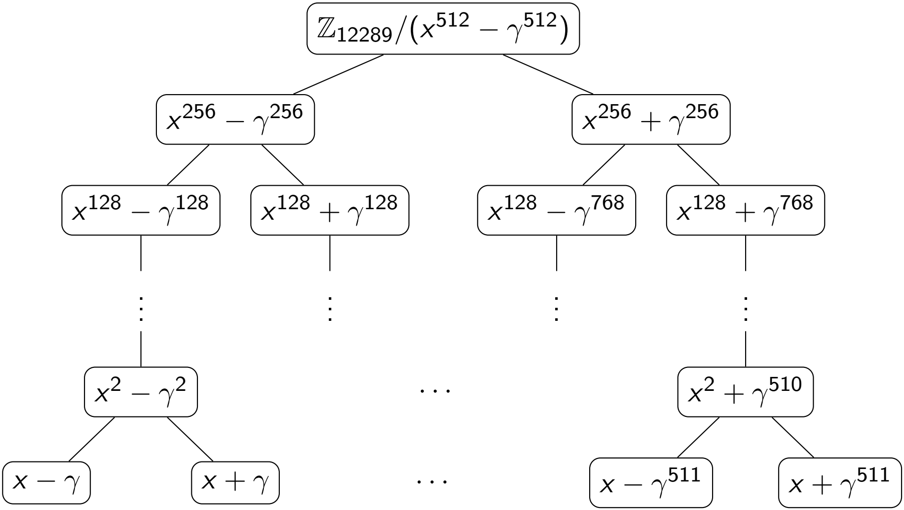
$$\mathbb{Z}_{12289}/(x^{512}+1) = \mathbb{Z}_q/(x^{512}-\gamma^{512})$$

$$\mathbb{Z}_{12289}/(x^{256}-\gamma^{256}) \qquad \mathbb{Z}_{12289}/(x^{256}+\gamma^{256})$$

CRT Map of NewHope512



CRT Map of NewHope512



CRT Map of NewHope-Compact512

Let $\gamma^{128} = -1 \mod 3329$.

$$\mathbb{Z}_{3329}/(x^{512}+1) \cong \mathbb{Z}_{3329}/(x^4-\gamma) \times \cdots \times \mathbb{Z}_{3329}/(x^4-\gamma^{127})$$

CRT Map of NewHope-Compact512

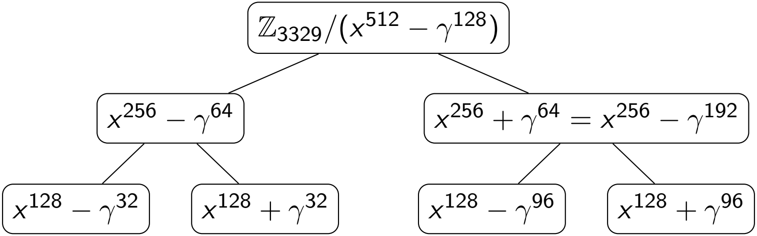
Let $\gamma^{128} = -1 \mod 3329$.

$$\mathbb{Z}_{3329}/(x^{512}+1) \cong \mathbb{Z}_{3329}/(x^4-\gamma) \times \cdots \times \mathbb{Z}_{3329}/(x^4-\gamma^{127})$$

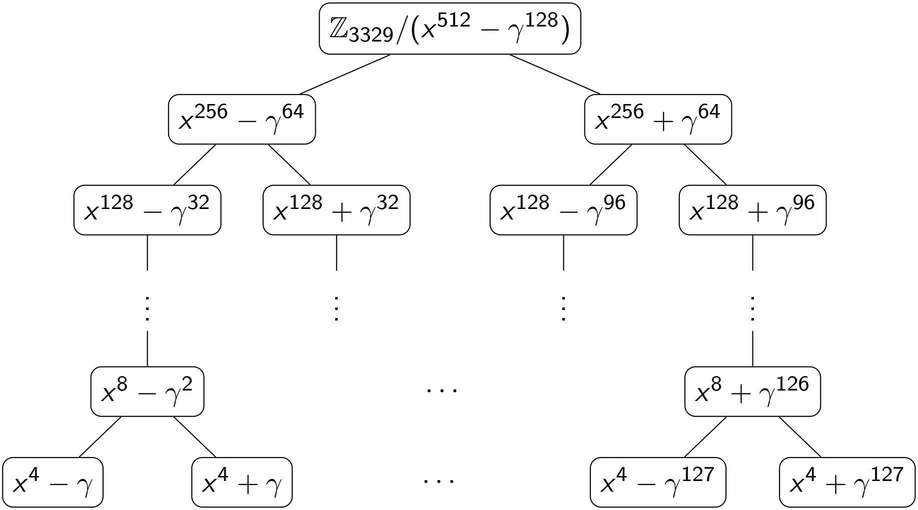
$$\mathbb{Z}_{3329}/(x^{512}+1) = \mathbb{Z}_{3329}/(x^{512}-\gamma^{128})$$

$$\mathbb{Z}_{3329}/(x^{256}-\gamma^{64}) \qquad \mathbb{Z}_{3329}/(x^{256}+\gamma^{64})$$

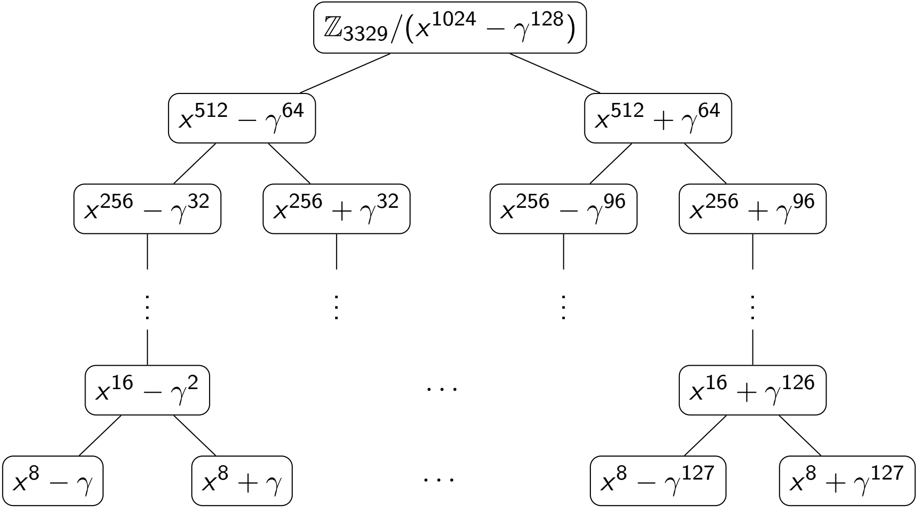
CRT Map of NewHope-Compact512



CRT Map of NewHope-Compact512



CRT Map of NewHope-Compact1024



Karatsuba Multiplication with Reduction

Let a, b and $c \in \mathbb{Z}_q/(X^4 - r)$ where $r = \gamma^i$.

function basemul(a, b)
  $d \leftarrow$ Apply One-Iteration Karatsuba[1] to get $d = a \cdot b$ where d is a degree 6 polynomial
  $c[0] \leftarrow d[0] + d[4] \cdot r$ ▷ $+$ and $\cdot$ for modular reduction
  $c[1] \leftarrow d[1] + d[5] \cdot r$
  $c[2] \leftarrow d[2] + d[6] \cdot r$
  $c[3] \leftarrow d[3]$
  return c
end function

[1] Weimerskirch and Paar, ePrint 2006/224

Computation Costs of Polynomial Multiplications

$\mathbb{Z}_{3329}/(x^{512}+1)$

Multiplication Methods \ Operations	# of Multiplications	# of Additions
Hybrid NTT-Schoolbook Multiplication	7808	12288
Hybrid NTT-Karatsuba Multiplication	7040	14592

Computation Costs of Polynomial Multiplications

$\mathbb{Z}_{3329}/(x^{512}+1)$

Multiplication Methods \ Operations	# of Multiplications	# of Additions
Hybrid NTT-Schoolbook Multiplication	7808	12288
Hybrid NTT-Karatsuba Multiplication	7040	14592

Method	Cycle counts ($\times 10^3$)
Schoolbook	21,7
Karatsuba	14,2

Parameter Sets

Table: Parameters of n=512

Parameter Set	NewHope512	NH-Compact512
Dimension n	512	512
Modulus q	12289	3329
Noise Parameter k	8	2

Table: Parameters of n=1024

Parameter Set	NewHope1024	NH-Compact1024
Dimension n	1024	1024
Modulus q	12289	3329
Noise Parameter k	8	2

Sizes in bytes

Parameter Set	512-CCA-KEM	
	NewHope	NewHope-Compact
$\|pk\|$	928	800
$\|sk\|$	1888	1632
$\|ciphertext\|$	1120	992

Parameter Set	1024-CCA-KEM	
	NewHope	NewHope-Compact
$\|pk\|$	1824	1568
$\|sk\|$	3680	3168
$\|ciphertext\|$	2208	2080

Cycle counts ($\times 10^3$) of C reference (non-optimized) implementations

Operations	CCA-KEM-512		
	Kyber	NewHope	NewHope-Compact
Gen	121.6	119.2	89.3
Encaps	164	180.2	147
Decaps	197.5	203.4	176.1
Total	483.1	502.8	412.4

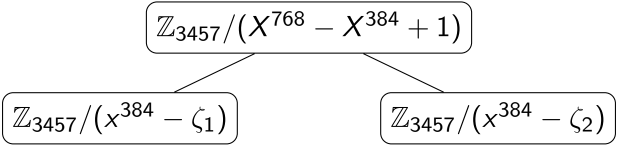
Operations	CCA-KEM-1024		
	Kyber	NewHope	NewHope-Compact
Gen	324.6	237.8	186.4
Encaps	381.4	365.2	321.8
Decaps	431.4	417.5	395
Total	1137.4	1020.5	902.2

Performed on Intel Skylake Core i7-6500U

NewHope-Compact768

Inspired by NTTRU [1]

$\mathbb{Z}_{3457}/(X^{768} - X^{384} + 1)$ and let ζ_1 and ζ_2 are two primitive sixth root of unity.



[1] Lyubashevsky and Seiler, CHES 2019

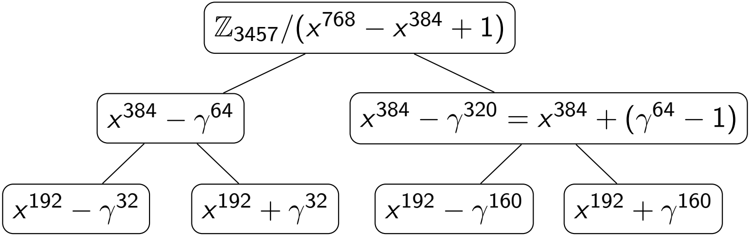
CRT Map of NewHope-Compact768

Let $\gamma^{384} = 1 \mod 3457$. Then, $\zeta_1 \equiv \gamma^{64} \mod 3457$ and $\zeta_2 \equiv \gamma^{320} \mod 3457$

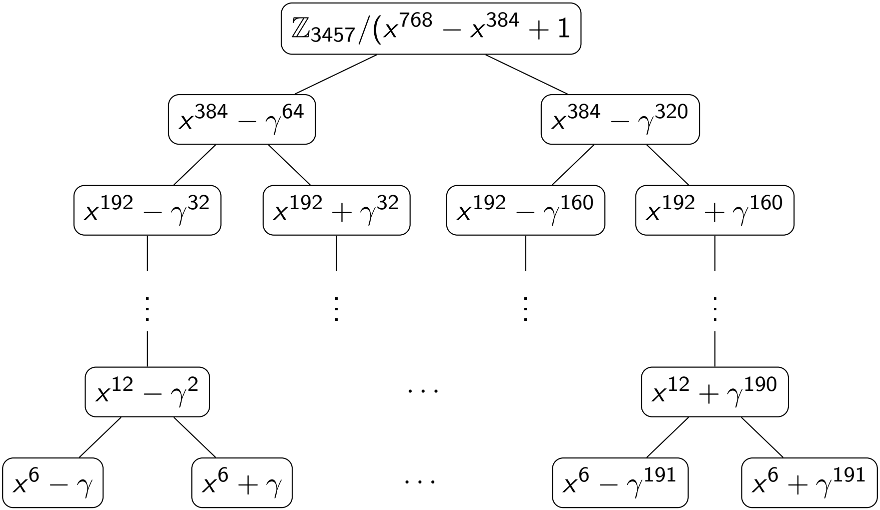
CRT Map of NewHope-Compact768

Let $\gamma^{384} = 1 \mod 3457$. Then, $\zeta_1 \equiv \gamma^{64} \mod 3457$ and $\zeta_2 \equiv \gamma^{320} \mod 3457$

$\zeta_1 + \zeta_2 = 1$



CRT Map of NewHope-Compact768



Cycle counts ($\times 10^3$) of C reference (non-optimized) implementations

Our ring is $\mathbb{Z}_{3457}/(X^{768} - X^{384} + 1)$

Operations	CCA-KEM-768		
	Kyber	NewHope	NewHope-Compact
Gen	208.8	-	137.9
Encaps	254.8	-	228.9
Decaps	294.7	-	277.8
Total	758.3	-	644.6

Performed on Intel Skylake Core i7-6500U

Future Works

- AVX2 implementation
- ARM Cortex-M4 implementation

Thank you

Source code available online at
www.github.com/erdemalkim/NewHopeCompact and
www.github.com/alperbilgin/NewHopeCompact.

y.alperbilgin@gmail.com