

# Analysis of Polynomial Multipliers for Post-quantum Schemes

*Sabrina Schunn*

Supervisor  
Aikata Aikata

# Relevance

Quantum Computers

Shor's algorithm

Severe Threat

Post-Quantum  
Cryptography

# Goals

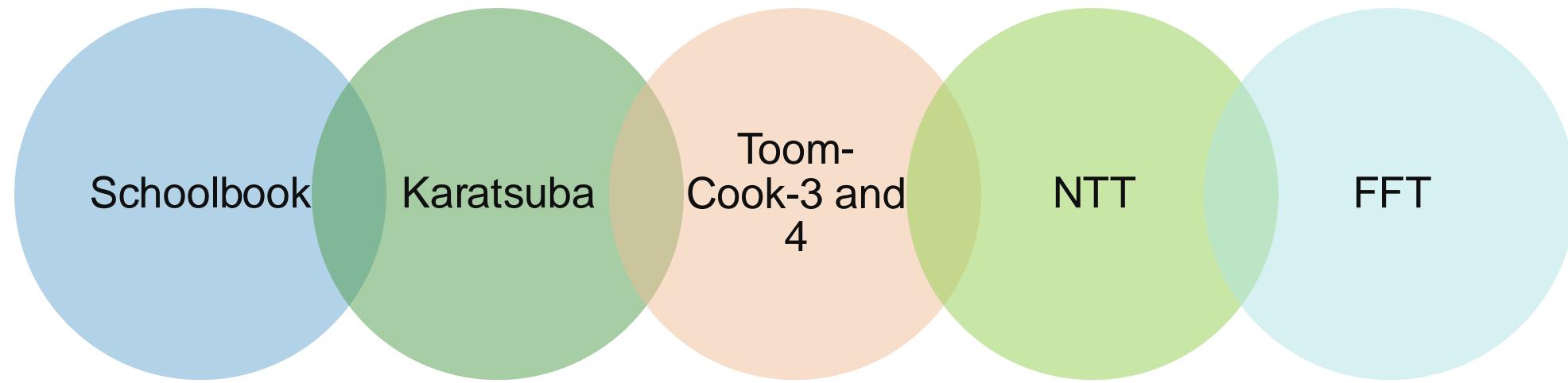
Implement...

Test...

Compare...

... Algorithms

# Polynomial Multiplication Algorithms

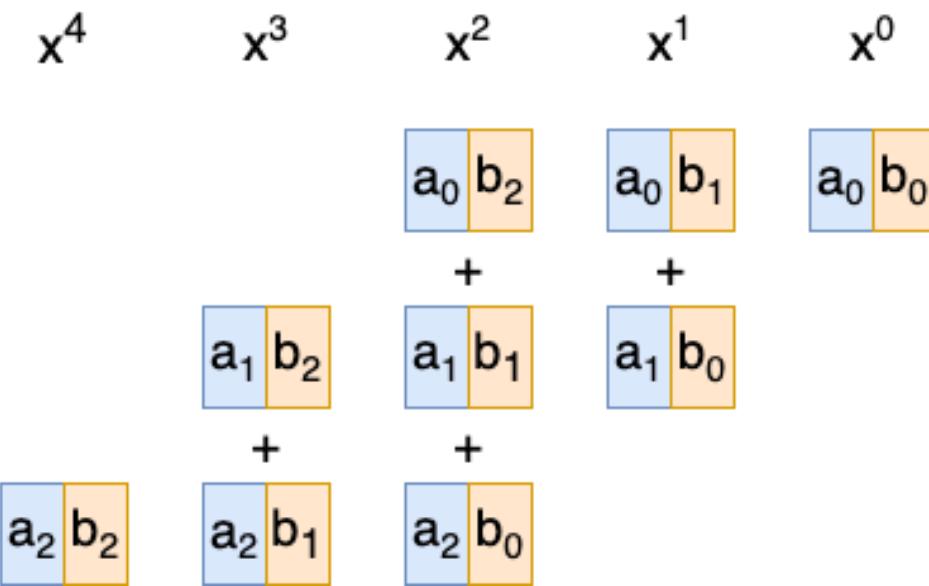


- Mathematical Background
- Runtime Complexities
- Advantages and Limitations
- Efficiency Considerations

# Schoolbook Multiplication

Runtime Complexity:  $\mathcal{O}(n^2)$

$$a \cdot b = (a_2 x^2 + a_1 x + a_0) \cdot (b_2 x^2 + b_1 x + b_0)$$



- + Straightforward
- + Simple
- Inefficient for bigger polynomials

# Karatsuba Multiplication

$$a \cdot b = (a_3 x^3 + a_2 x^2 + a_1 x + a_0) \cdot (b_3 x^3 + b_2 x^2 + b_1 x + b_0)$$

y      w  
y      w

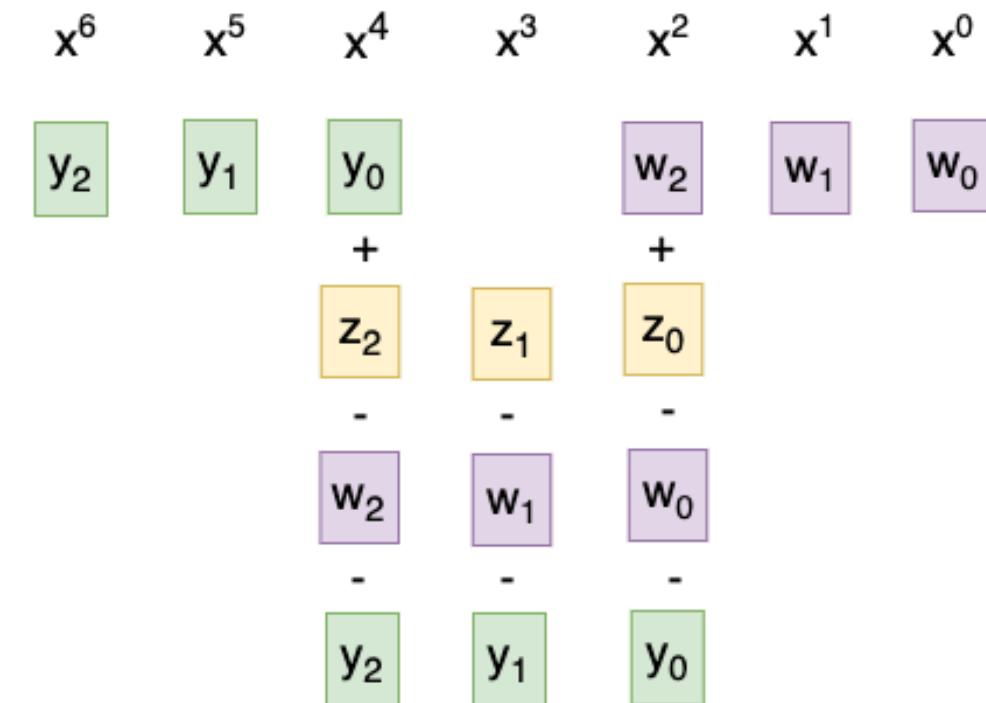
Runtime Complexity:

$$\mathcal{O}(n^{\log_2(3)}) \approx \mathcal{O}(n^{1.58})$$

+ Recursion

+ Multithreading

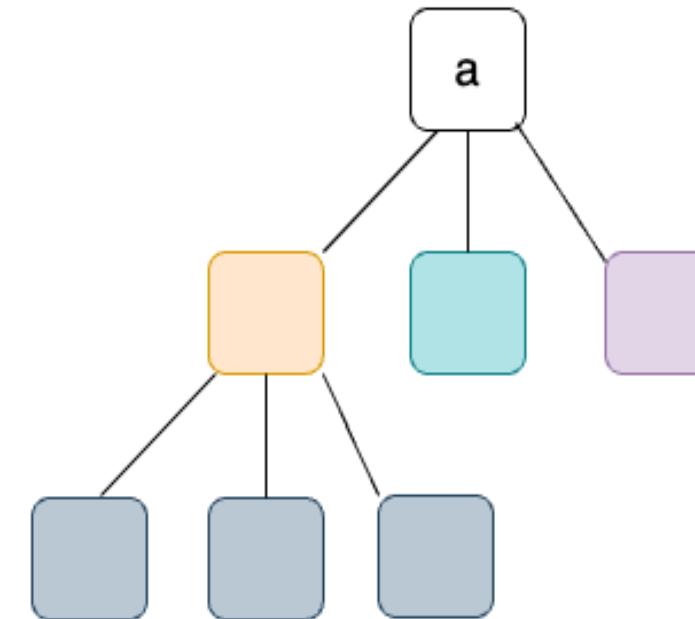
- Recursion Depth



# Toom-Cook Multiplication

- Splitting
- Evaluation
- Pointwise Multiplication
- Interpolation
- Recomposition
- Toom-3:  $\mathcal{O}(n^{\log_3(5)}) \approx \mathcal{O}(n^{1.47})$
- Toom-4:  $\mathcal{O}(n^{\log_4(7)}) \approx \mathcal{O}(n^{1.40})$

$$a = ( \boxed{a_8}x^8 + \boxed{a_7}x^7 + \boxed{a_6}x^6 + \boxed{a_5}x^5 + \boxed{a_4}x^4 + \boxed{a_3}x^3 + \boxed{a_2}x^2 + \boxed{a_1}x + \boxed{a_0} )$$



# Toom-Cook Multiplication

- + Efficiency
- + Combinations
- Restrictions of q
- Overhead

---

**Algorithm 3** Toom-3 Interpolation Sequence

---

```
init tmp1 ← (r(-2) - r(1))/3
init tmp2 ← (r(1) - r(-1))/2
init tmp3 ← r(-1) - r(0)
c(0) ← r(0)
c(4) ← r(∞)
c(3) ← (tmp3 - tmp1)/2 + 2c(4)
c(2) ← tmp3 + tmp2 - c(4)
c(1) ← tmp2 - c(3)
```

---

# NTT – Number Theoretic Transform

- Normal Domain  $\rightarrow$  NTT Domain

$$a = \boxed{\textcolor{blue}{x}} + \boxed{\textcolor{blue}{x}} \quad b = \boxed{\textcolor{yellow}{x}} + \boxed{\textcolor{yellow}{x}} \quad \text{root} = \boxed{\textcolor{red}{1}} \quad \text{root}^{-1} = \boxed{\textcolor{violet}{1}}$$

- Primitive Root:  $a^k \equiv 1 \pmod{q}$

$$\text{NTT}(a) = \boxed{\textcolor{blue}{x}} \boxed{\textcolor{red}{1}} + \boxed{\textcolor{blue}{x}} \boxed{\textcolor{red}{1}} + \boxed{\textcolor{blue}{x}} \boxed{\textcolor{red}{1}} + \boxed{\textcolor{blue}{x}} \boxed{\textcolor{red}{1}}$$

- Forward transformation:  $\mathcal{O}(n^2)$

$$\text{NTT}(a) \circ \text{NTT}(b) = \boxed{\textcolor{green}{x}} + \boxed{\textcolor{green}{x}} + \boxed{\textcolor{green}{x}} + \boxed{\textcolor{green}{x}}$$

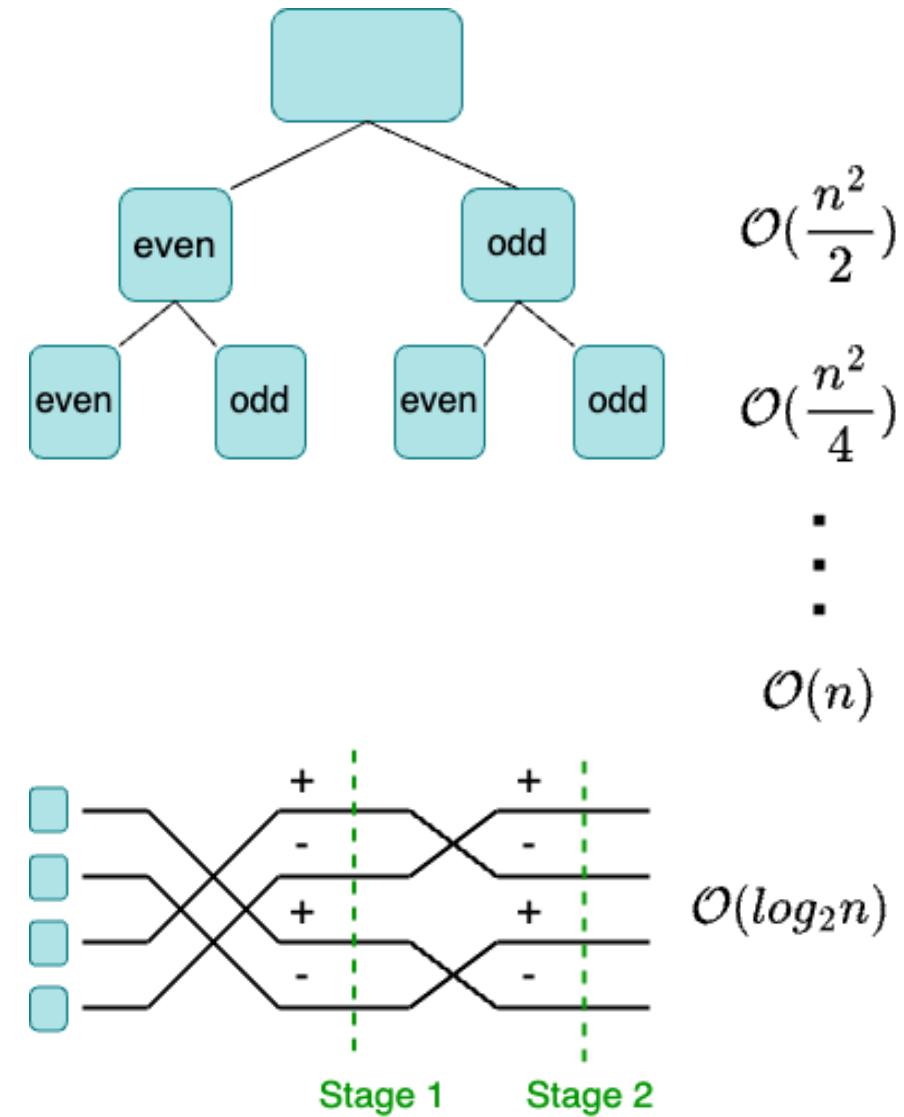
$$\text{NTT}^{-1}(\text{NTT}(a) \circ \text{NTT}(b)) = \boxed{\textcolor{green}{x}} \boxed{\textcolor{violet}{1}} + \boxed{\textcolor{green}{x}} \boxed{\textcolor{violet}{1}} + \boxed{\textcolor{green}{x}} \boxed{\textcolor{violet}{1}} + \boxed{\textcolor{green}{x}} \boxed{\textcolor{violet}{1}}$$

# FFT – Fast Fourier Transform

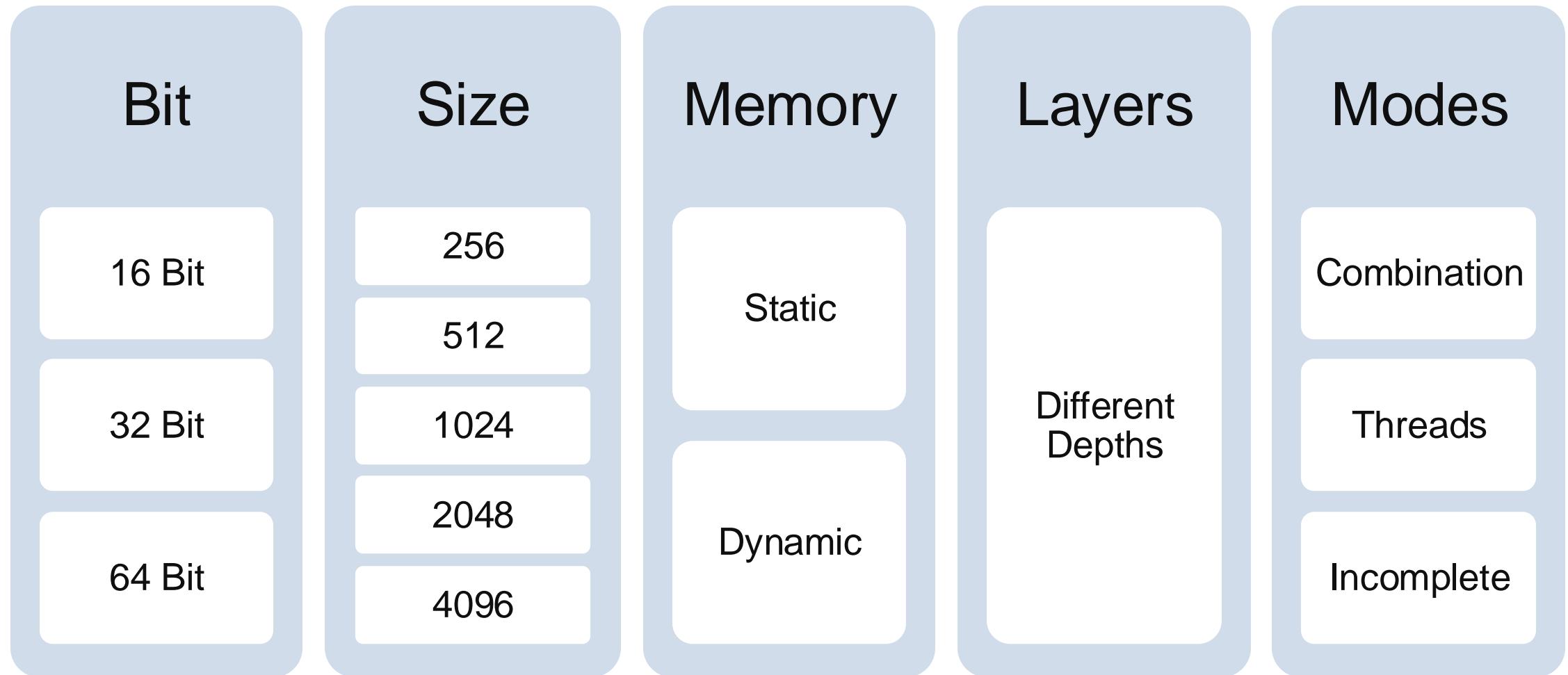
- Forward Transform: **Cooley-Tukey**
- Inverse Transform: **Gentleman-Sande**
- Twiddle Factors & Butterfly Operations

Runtime Complexity:  $\mathcal{O}(n \log n)$

- + Efficiency, Incomplete Version
- Restrictions, Overhead

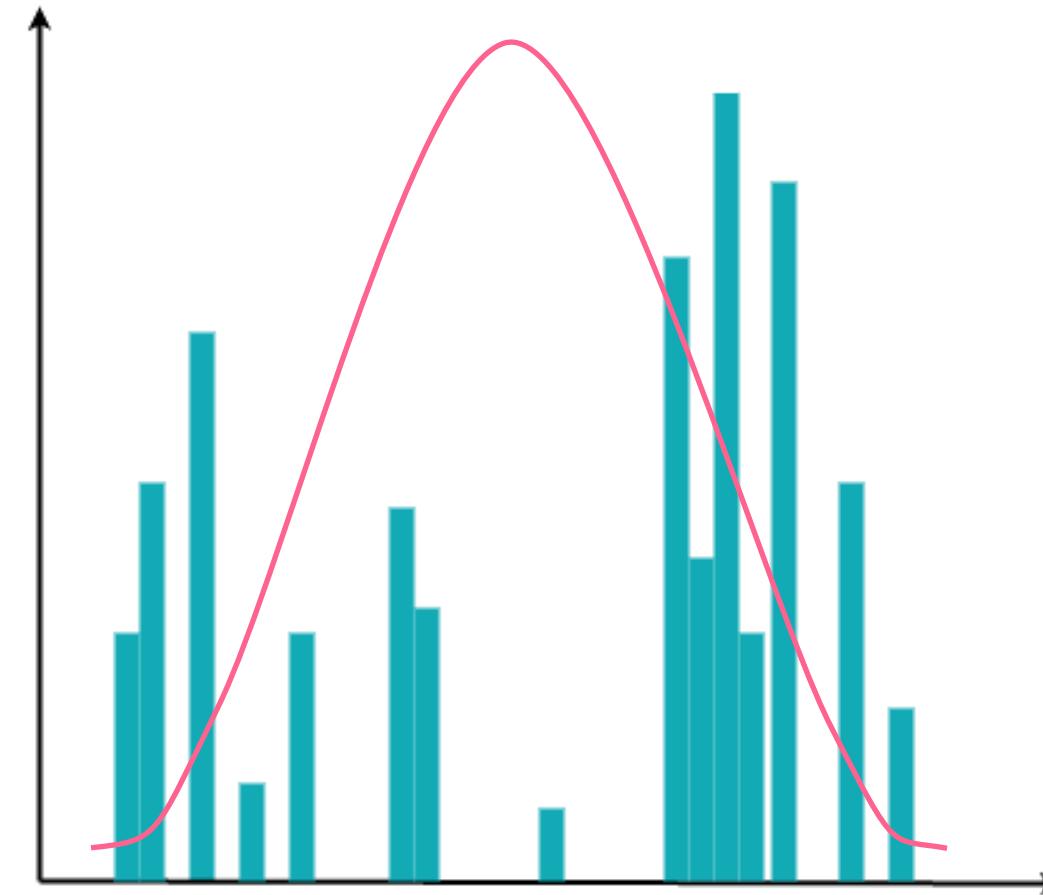


# Testing Methodology



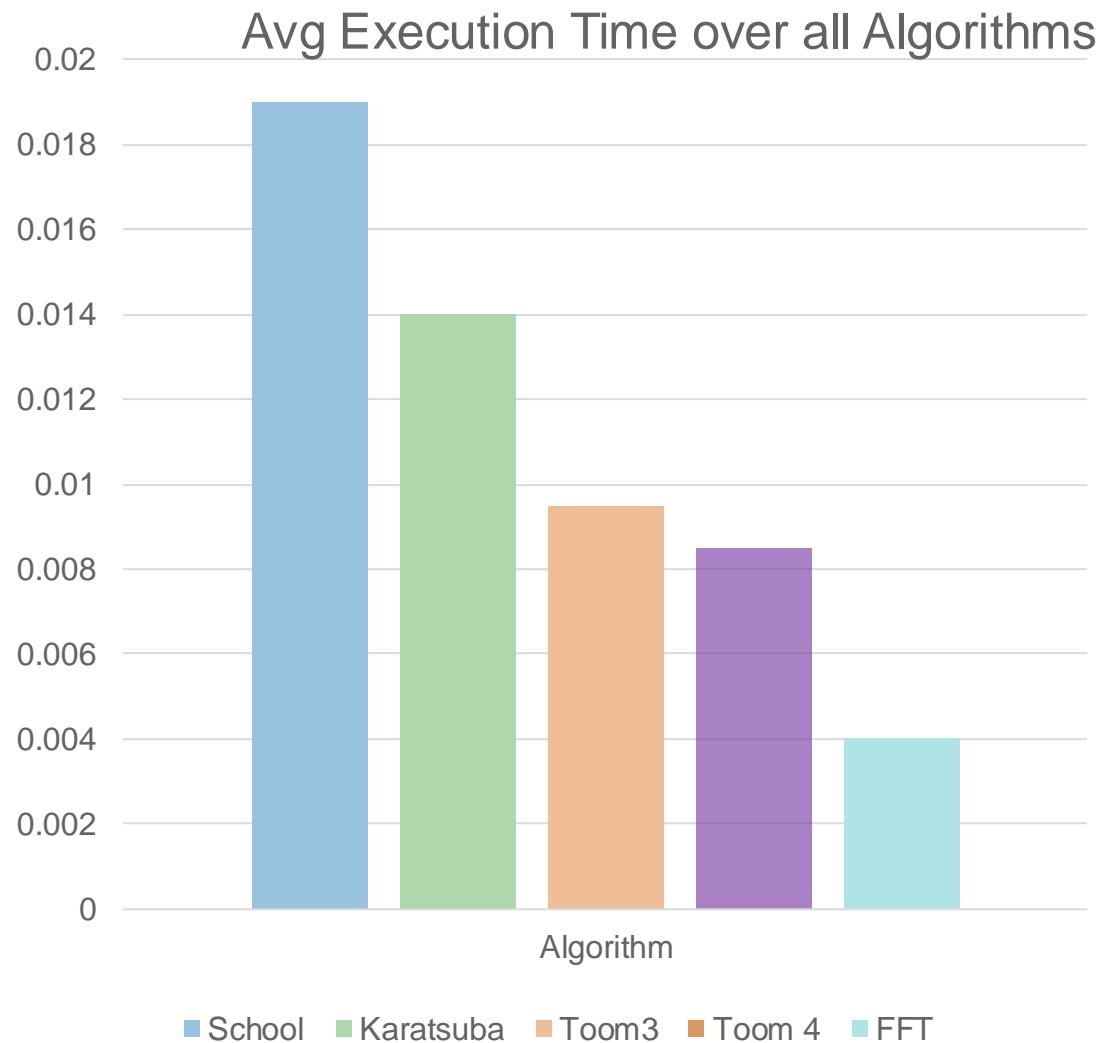
# Data Processing

- **Anderson-Darling Test**
- **Mann-Whitney U Test**
- **Kruskal-Wallis Test**
- Post hoc: **Dunn Test**
- P-value
- Pairwise comparison



# Results

Algorithm	Speedup
school	1.00 x
karatsuba	1.29 x
toom3	2.00 x
toom4	2.23 x
fft	6.75 x



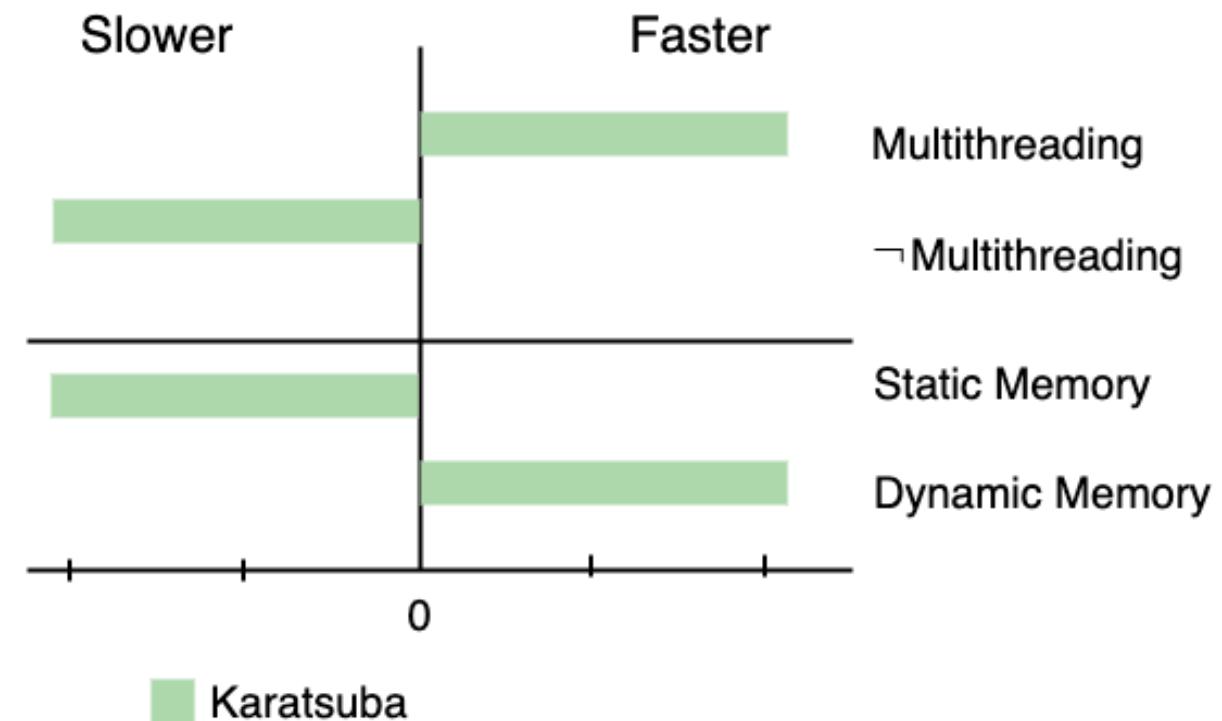
# Multithreading & Memory Allocation

# Karatsuba:

- Multithreading faster
  - Polynomial size = 256  
  - Dynamic Memory allocation faster
  - Polynomial size = 256
  - Implementation specific

# Toom-Cook:

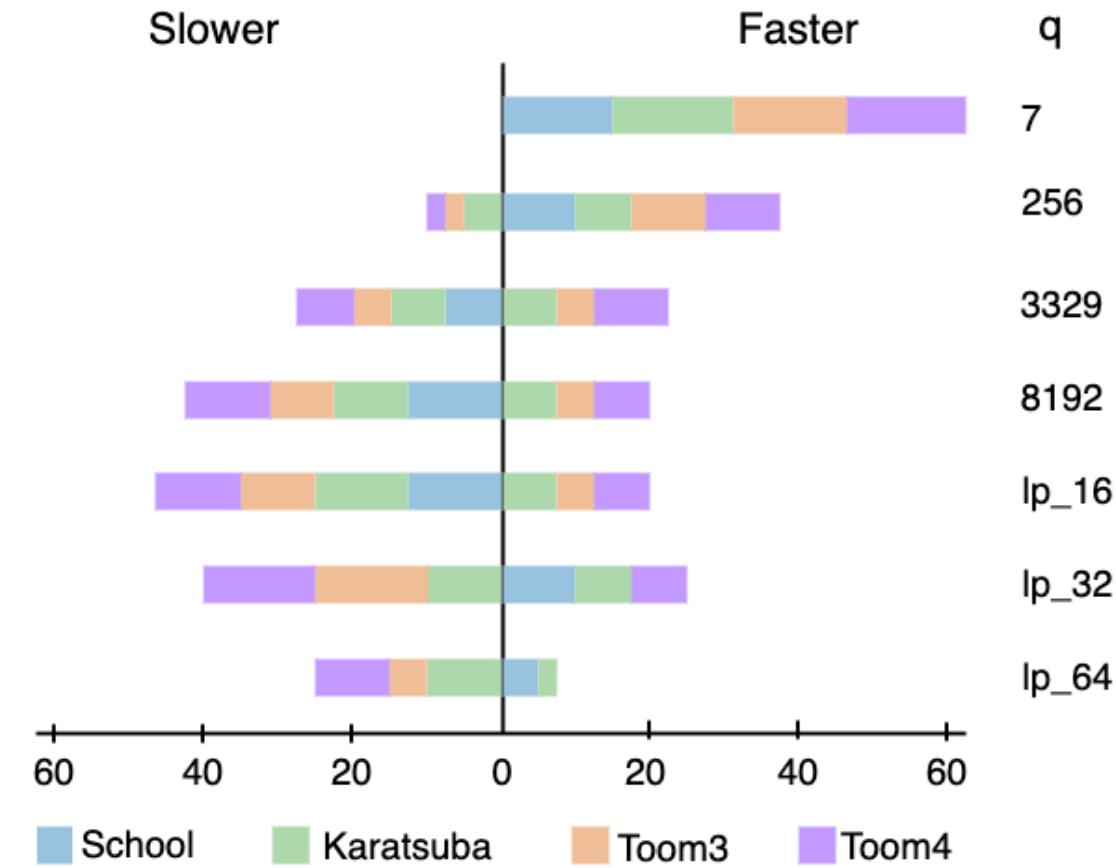
- No Difference



# Effect of modulus q

## All tested Algorithms:

- Smaller numbers faster
- Moderate to large numbers slower



# Effect of Bit sizes

## Toom-3:

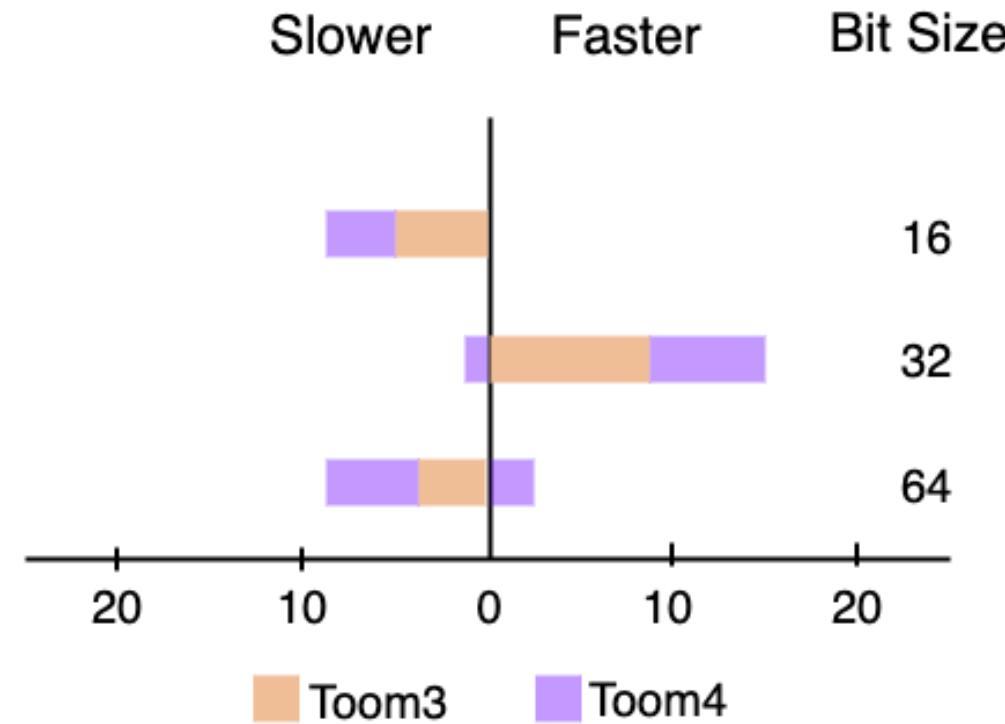
- 32 Bit faster
- 16 Bit and 64 Bit slower

## Toom-4:

- 32 Bit faster
- 16-Bit and 64 Bit slower
- 64 Bit outlier

## Schoolbook, Karatsuba and FFT:

- No difference



# Effect of Recursion

## Toom-3:

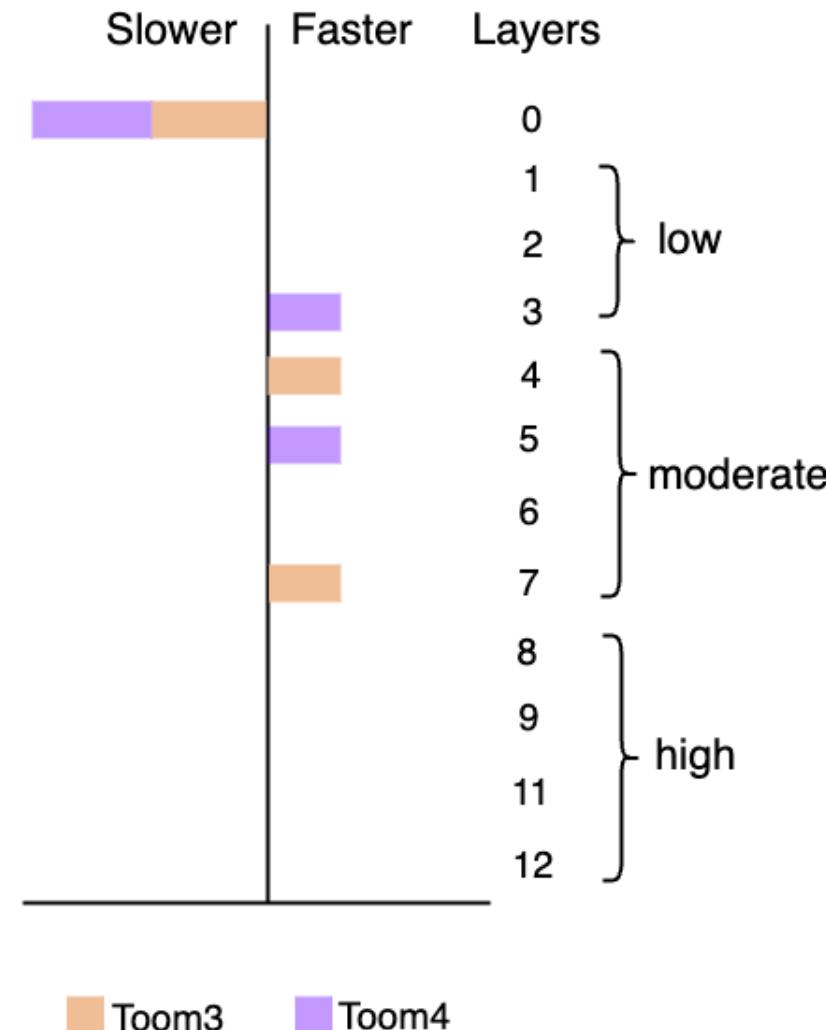
- Moderate recursion faster
- No Recursion slower

## Toom-4:

- Moderate recursion faster
- No Recursion slower

## Karatsuba:

- No differences



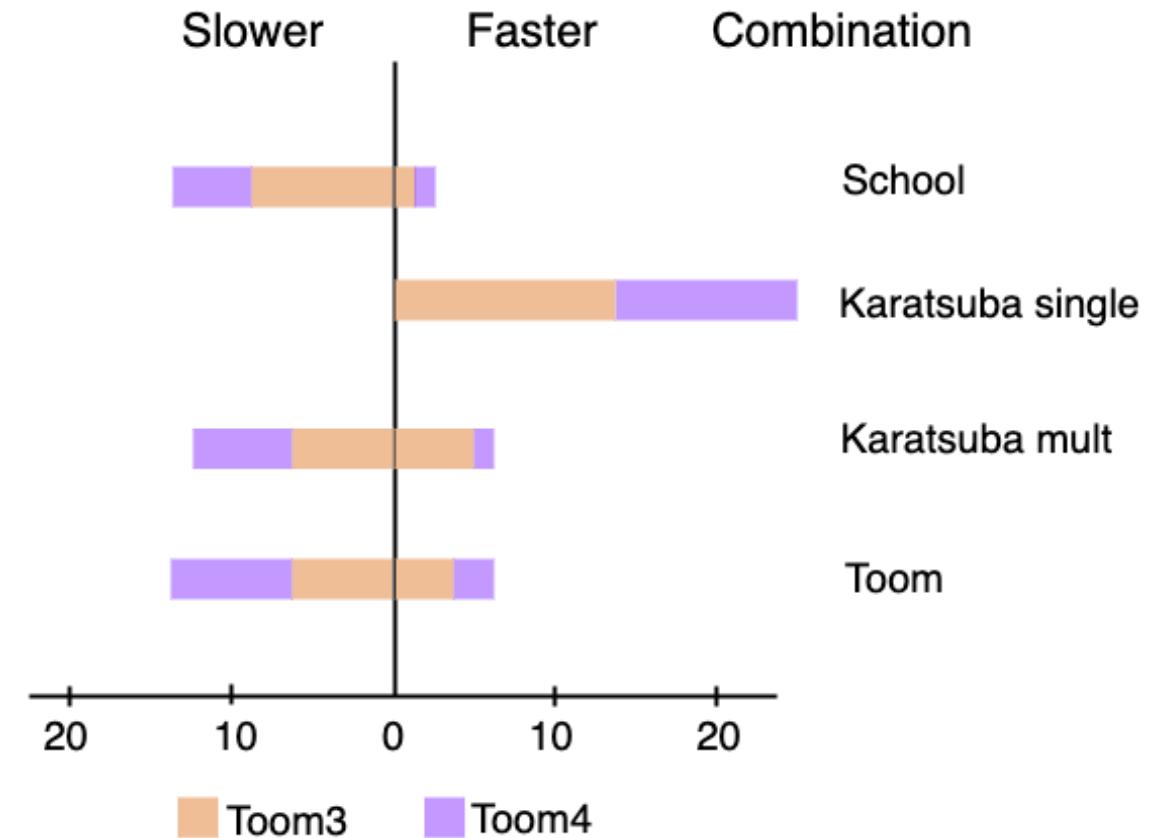
# Effect of Combination

## Toom-3:

- Toom3 + Karatsuba faster
- Other combination modes slower

## Toom-4:

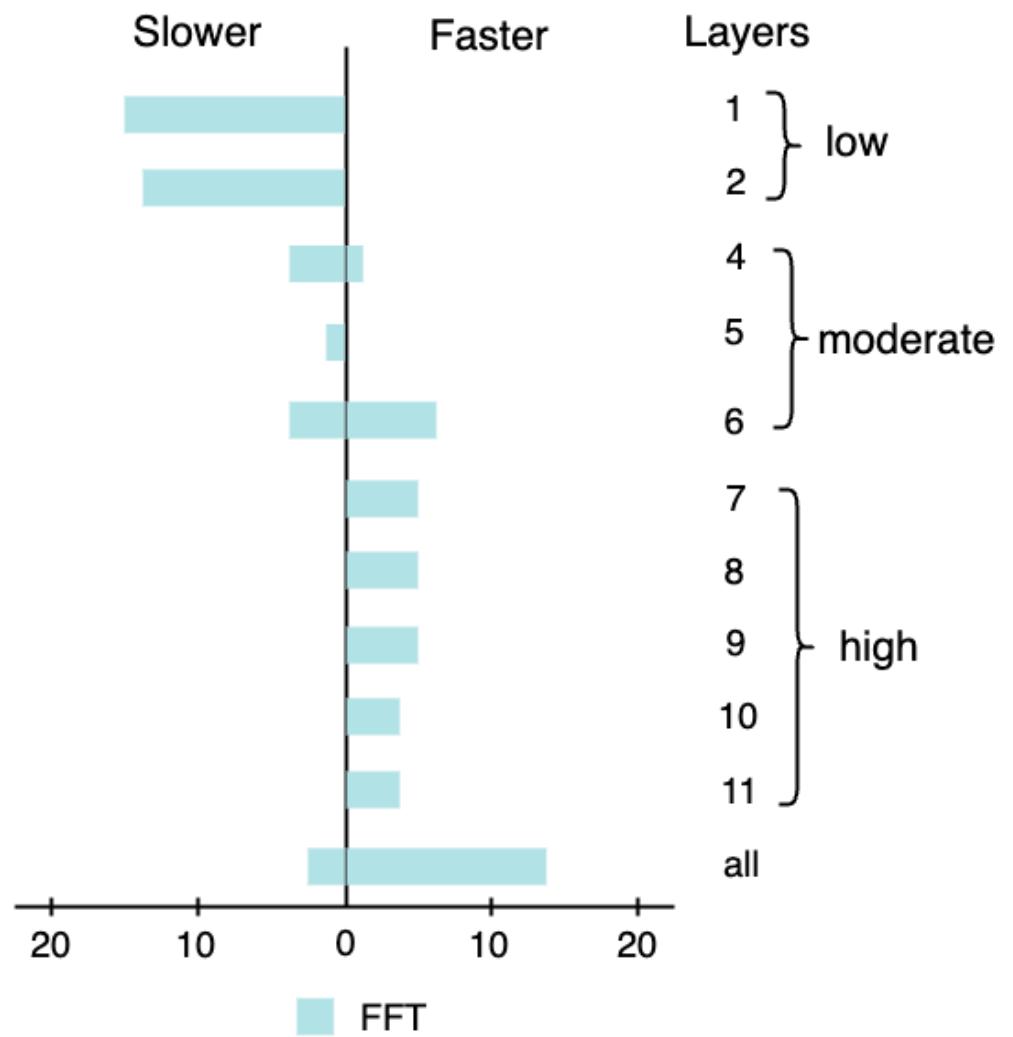
- Toom4 + Karatsuba faster
- Other combination modes slower



# Effect of Incompleteness

## FFT:

- No incompleteness faster
- High number of layers faster
- Moderate number of layers slower
- Low number of layers slowest



# Conclusion

General

## Schoolbook

- Small input size
- Small overhead

## Karatsuba

- Moderate input size
- Moderate overhead

## Toom-Cook

- Moderate input size
- Moderate overhead
- Restrictions

## FFT

- Large input size
- Restrictions

Specific

- Small q faster
- Moderate q slower
- Large q slower
- Bit size no effect

- Small q faster
- Moderate q slower
- Large q slower
- Multithreading faster
- Bit size no effect
- Recursion no effect

- Small q faster
- Moderate q slower
- Large q slower
- 32 Bit faster
- 16 and 64 Bit slower
- Moderate recursion faster
- No recursion slower
- Toom + Karatsuba faster

- Bit size no effect
- Complete version faster
- High number layers faster
- Moderate/low number layers slower

# Analysis of Polynomial Multipliers for Post-quantum Schemes

*Sabrina Schunn*

Supervisor  
Aikata Aikata