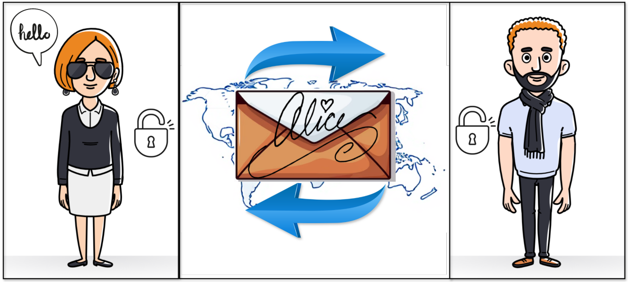
Polynomial Arithmetic Tools

Dennis Günter Köb
Supervisor: Aikata Aikata

12.6.2025

SCIENCE
PASSION
TECHNOLOGY

Introduction: Quantum Computers and Cryptography



Multiplication Comparison [Kan]

Technique	**Constraints on q**	**Constraints on n**
Schoolbook	None	None
Karatsuba	None	Divisible by 2
NTT	Primitive $2n$-th root of unity in $\mathbb{Z}_q$	Power of 2

Ring Example

Multiplication in $\mathbb{Z}_7[x]/(x^3+1)$

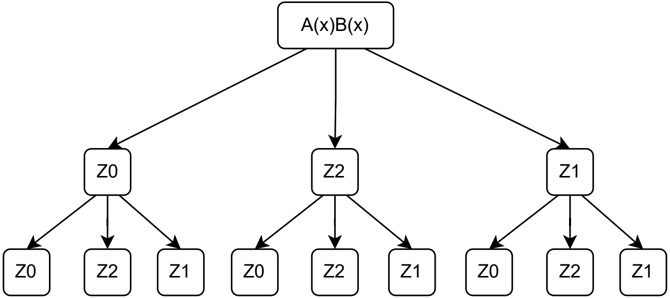
$$(1x^2+2x+3)\cdot(4x^2+5x+6)$$

	x^4	x^3	x^2	$x^1, -x^4$	$x^0, -x^3$
			$3\cdot4\equiv5$	$3\cdot5\equiv1$	$3\cdot6\equiv4$
		$2\cdot4\equiv1$	$2\cdot5\equiv3$	$2\cdot6\equiv5$	
	$1\cdot4\equiv4$	$1\cdot5\equiv5$	$1\cdot6\equiv6$		
					$2\cdot4\equiv1$
				$1\cdot4\equiv4$	$1\cdot5\equiv5$
			$14\equiv0$	$2\equiv2$	$-2\equiv5$

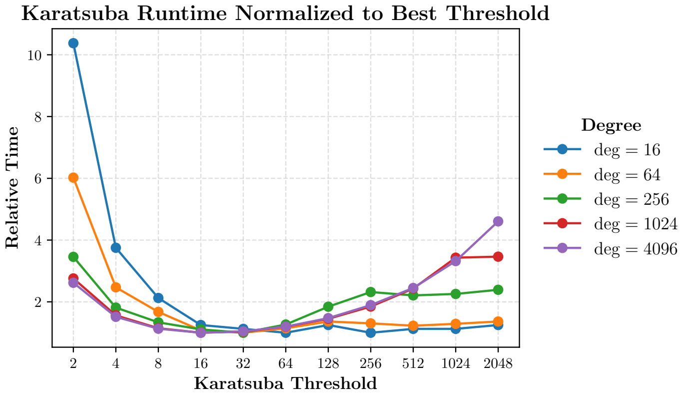
$$0\,x^2\;+\;2\,x\;+\;5$$

Karatsuba

Split into 3 multiplications: $O(n^{1.585})$

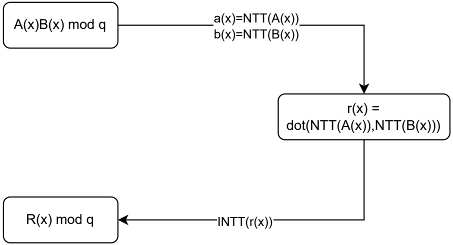


Karatsuba Recursion

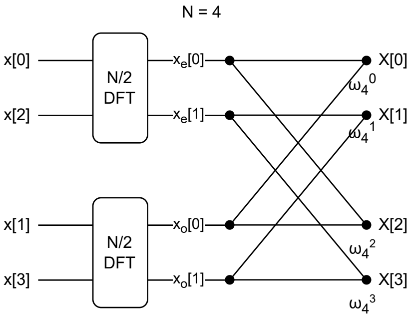


Number-Theoretic Transform (NTT)

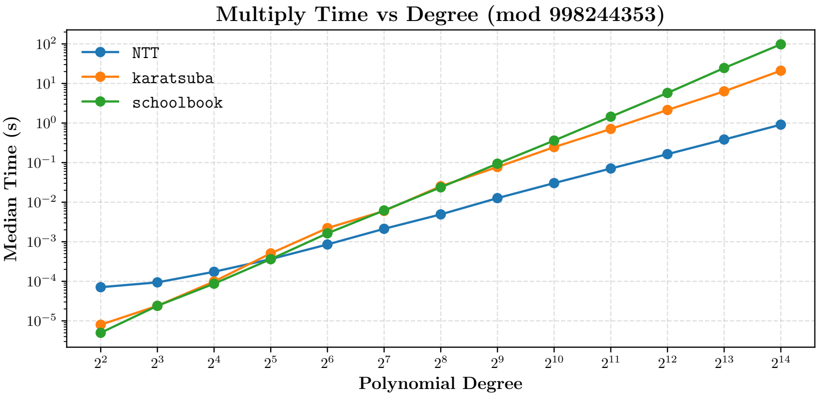
- Analagous to the DFT.
- FFT like acceleration possible. $\approx O(n \log(n))$



NTT with Cooley-Tukey Butterfly



Multiplication Comparison



Modular Reduction: overview

- Division-based
- Barrett
- Mongomery
- Mersenne and Pseudo-Mersenne primes

Division-based Reduction

- Division instructions are slow [Fog23].
- Avoid at all costs.

Barrett Reduction

- Precomputes a constant $m = \lfloor 2^k / q \rfloor$ to approximate division.
- Avoids division during runtime by replacing it with shifts and multiplications.

Montgomery Reduction

- Avoids division by transforming into a special "Montgomery domain."
- Uses $R = 2^k$, where $k > \log_2(q)$, to simplify calculations.
- Efficient for large q, but requires q coprime with R.
- Example:

$$T \bmod q \quad \text{is computed as} \quad (T + m \cdot q)/R$$

Mersenne Prime Reduction

$$\text{If } q = 2^k - 1 : \quad x \bmod q \;=\; \left(\, x \,\&\, (2^k - 1)\,\right) \;+\; \big(x \gg k\big).$$

- Since $2^k \equiv 1 \pmod{q}$, each "high-bits" chunk adds back to the low part.
- If the sum $\big((x \,\&\, (2^k - 1)) + (x \gg k)\big)$ still $\geq q$, subtract q once more.
- Example: $q = 31 = 2^5 - 1,\ x = 45$:

$$45 \bmod 31 = (\, 45 \,\&\, 31) + (45 \gg 5) = (13) + (1) = 14.$$

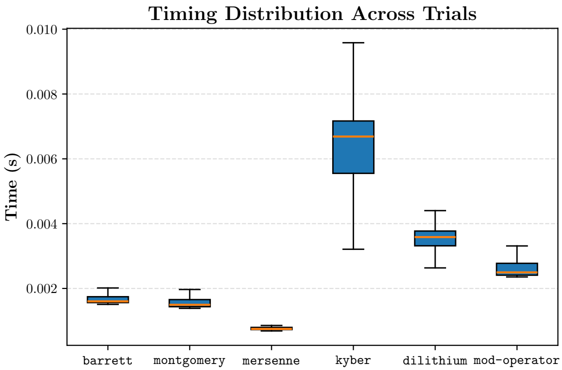
Dilithium Pseudo-Mersenne Reduction [AMI+23]

If $q = 2^{23} - 2^{13} + 1 \;\Rightarrow\; 2^{23} \equiv 2^{13} - 1 \pmod{q}$,

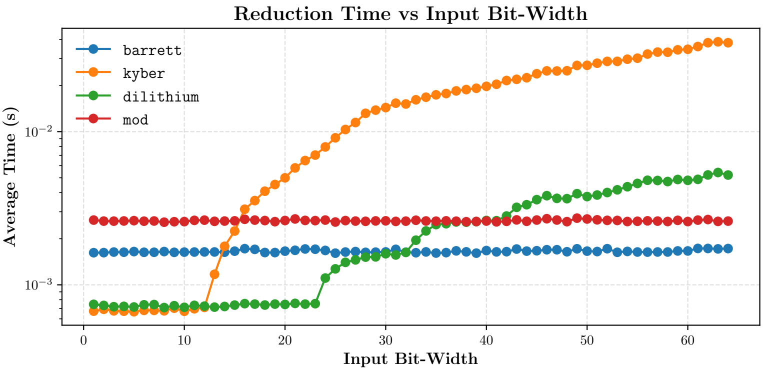
Require: x ▷ integer to reduce

while $x \gg 23 \neq 0$ **do**
    $\mathrm{hi} \leftarrow x \gg 23$
    $\mathrm{lo} \leftarrow x \,\&\, ((1 \ll 23) - 1)$
    $x \leftarrow \mathrm{lo} \;+\; (\mathrm{hi} \ll 13) \;-\; \mathrm{hi}$
end while
if $x \;\geq\; 8380417$ **then**
    $x \leftarrow x - 8380417$
end if
return x

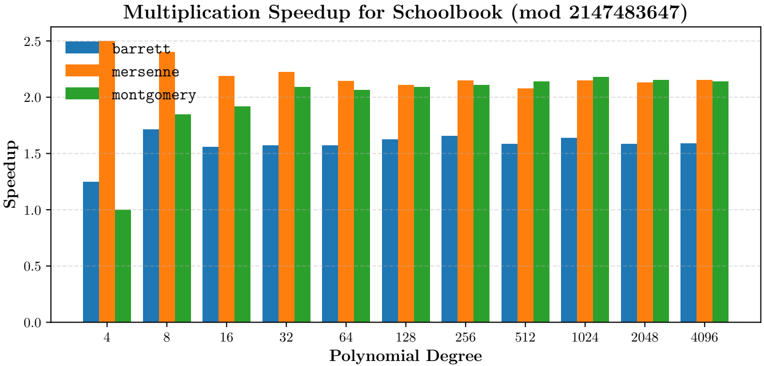
Modular Reduction comparison



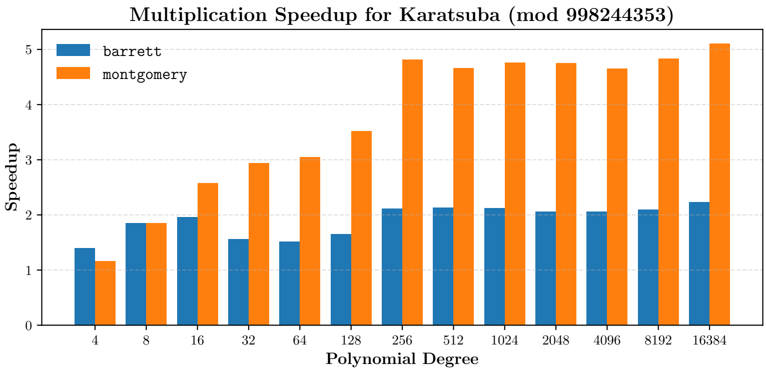
Modular Reduction comparison



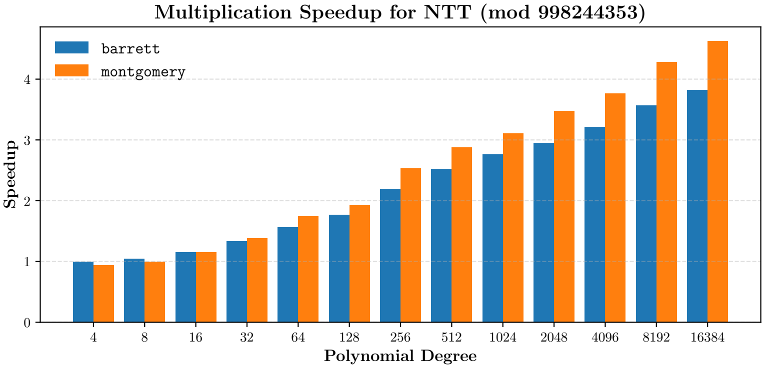
Modular Reduction Results: Schoolbook



Modular Reduction Results: Karatsuba



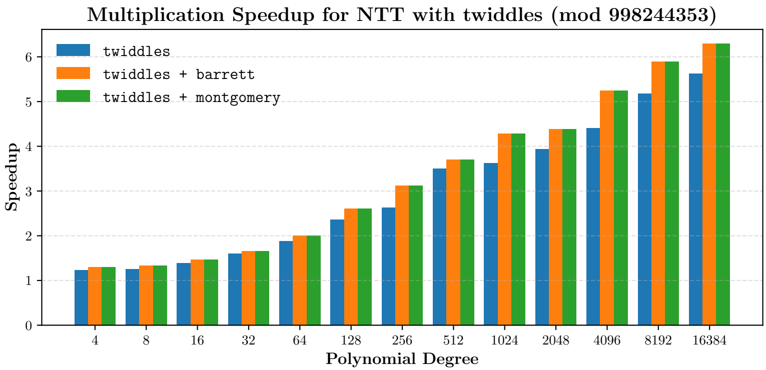
Modular Reduction Results: NTT



Twiddle Precomputation

1. Twiddles can be precomputed for (n, q, ω)
2. For montgomery they can be computed in montgomery-form.

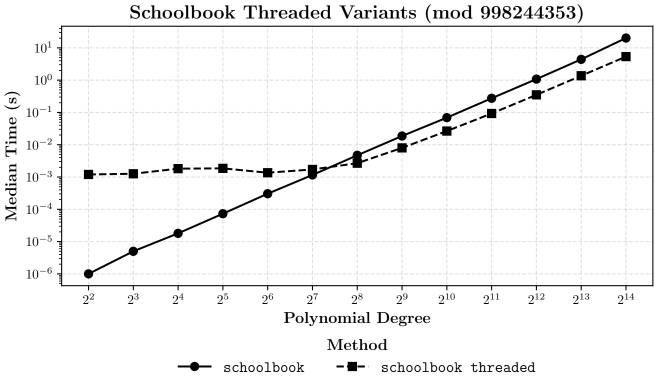
Modular Reduction Results: NTT + Twiddles



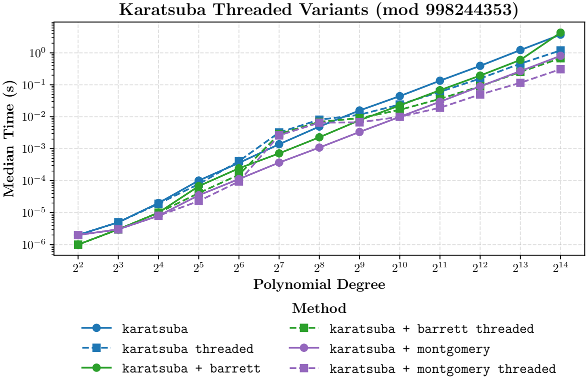
Multithreading

1. For each method split the workload.
2. For recursive calls turn function call into a thread.

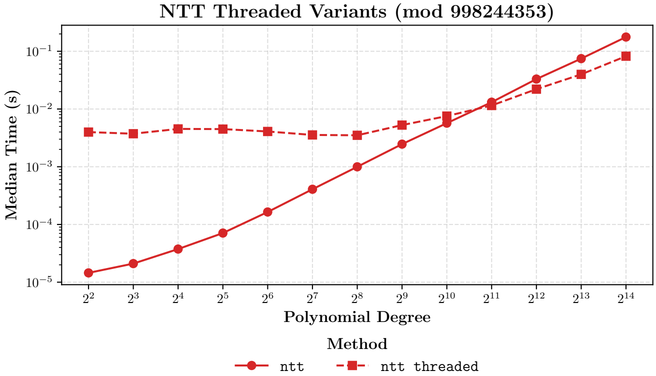
Multithreading: Schoolbook



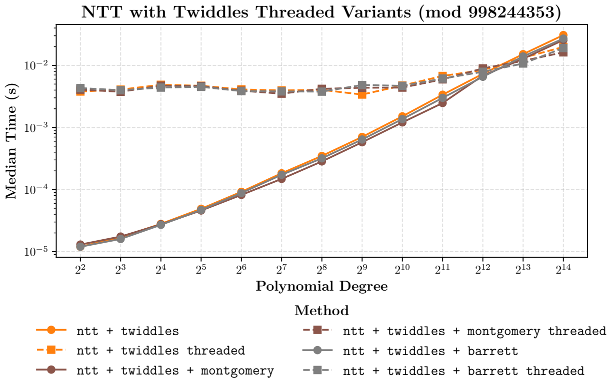
Multithreading: Karatsuba



Multithreading: NTT



Multithreading: NTT + Twiddles



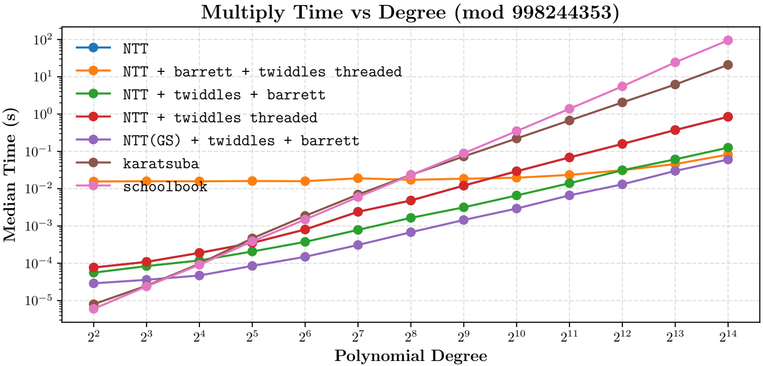
Tool Capabilities

- Basic polynomial Arithmetic
- Variety of multiplication and reduction techniques.
- Support for testing.

Further Improvements and Future Work

- Montgomery only lift one operand into representation. [Sei18].
- CPU Specifics: AVX2 vectorization.
- Avoiding memory allocations.
- Gentleman-Sande butterfly for INTT.
- Branchless code.

Summary: Results



References I

[AMI+23] Aikata Aikata, Ahmet Can Mert, Malik Imran, Samuel Pagliarini, and Sujoy Sinha Roy. **KaLi: A Crystal for Post-Quantum Security Using Kyber and Dilithium.** *IEEE Transactions on Circuits and Systems I: Regular Papers* 70.2 (Feb. 2023). Conference Name: IEEE Transactions on Circuits and Systems I: Regular Papers, pp. 747–758. ISSN: 1558-0806. DOI: 10.1109/TCSI.2022.3219555. URL: https://ieeexplore.ieee.org/abstract/document/9946370 (visited on 11/17/2024).

References II

[Fog23] Agner Fog. **Instruction Tables: Lists of instruction latencies, throughputs and micro-operation decomposition.** https://www.agner.org/optimize/instruction_tables.pdf. Accessed: 2025-06-01. 2023.

[Kan] Matthias J Kannwischer. **Polynomial Multiplication for Post-Quantum Cryptography.** en ().

[Sei18] Gregor Seiler. **Faster AVX2 optimized NTT multiplication for Ring-LWE lattice cryptography.** Cryptology ePrint Archive, Paper 2018/039. 2018. URL: https://eprint.iacr.org/2018/039.