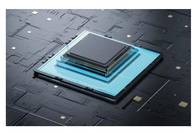
Multiplying Not-So-Big Integers with FFTs

Finding the Crossover Point on Large Modern OoO ARM CPUs

Cesare Huang[1], Daisy Meng-Wei Liu[1, 2], David Shu-Yu Wu[1, 3], Bow-Yaw Wang[1], and Bo-Yin Yang[1]
[1] IIS and CITI, Academia Sinica, Taipei, Taiwan
[2] National Tsing Hua University, Hsinchu, Taiwan [3] National Taiwan University, Taipei, Taiwan
Email: byyang@iis.sinica.edu.tw

Motivation

From where can NTT be faster than other multiplications?



Cortex-M3 and Cortex-M55

Becker et al. : 2048 bits



Cortex-A76

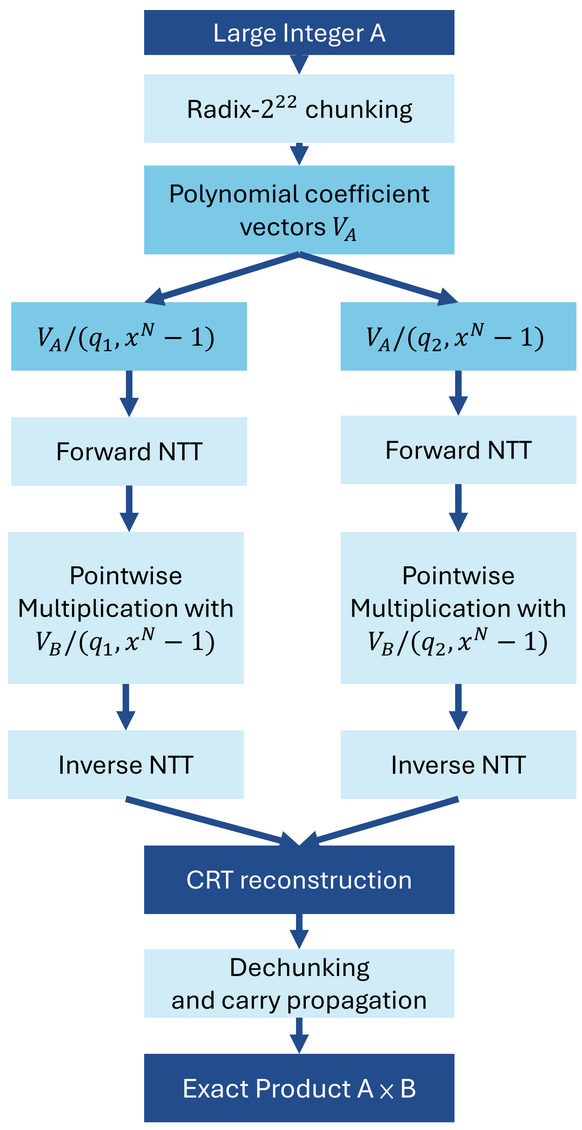
?

Contribution

- **Multiplication :** Build Neon-optimized NTT multipliers for 5632-, 8448-, 11264-, 14080-bit operands, and evaluate them against tuned-GMP on Cortex-A76.
- **Montgomery Multiplication and OpenSSL RSA :** Integrate the NTT multipliers into OpenSSL's Montgomery path with fixed-operand precomputation.
- **Formal Verification :** Check the core Neon kernels with CryptoLine and HOL Light for algebraic correctness and range safety.

Methodology

Workflow



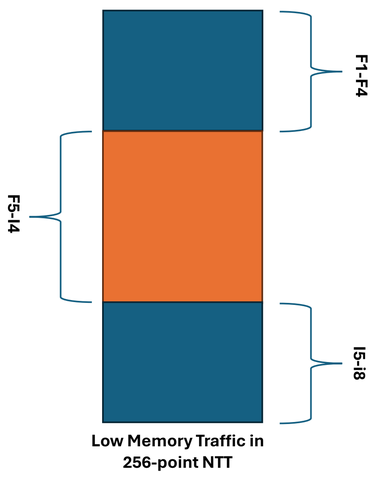
* Another large integer B undergoes the same chunking and forward-NTT pipeline; its transformed coefficients are omitted here for simplicity.

Implementation Optimizations

Zero-Skipping

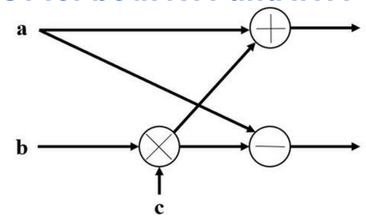
- Specialize radix-3 NTT to employ padded zeroes in the 3 x 256 Good-Thomas layouts.

Layer Fusion



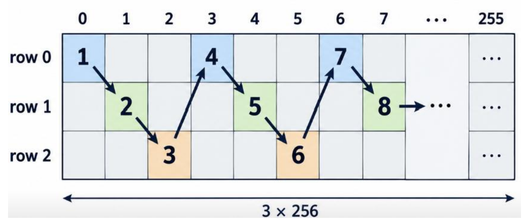
Low Memory Traffic in 256-point NTT

CT for both NTT and iNTT



Friendly output bound
Fewer lazy reductions

Dechunking in Good's Layout



Free Inverse Permutation

Parameter Table

Operand Size	NTT Length	Decomposition
5632 bits	512	Radix-2
8448 bits	768	3x256 Good–Thomas

Results

Large Integer Multiplication

Bits	GMP (Vari.-time)	Ours	
5632	22903	21472	**+6.25%**
8448	41051	34212	**+16.66%**

Montgomery Multiplication

Multiplier	Bits	OpenSSL Neon	Ours	
5632	5120	56597	47190	**+16.62%**
8448	6144	80227	76061	**+5.19%**
	8192	139720	77683	**+44.40%**

- **Crossover:** The practical crossover against GMP is below 5632 bits.

OpenSSL RSA

Multiplier	Bits	Operation	OpenSSL	Ours	
5632	5120	Verify	1413966	1070065	**+24.32%**
		Encrypt	1419155	1076692	**+24.13%**
8448	6144	Verify	2029822	1703906	**+16.06%**
		Encrypt	2035934	1710650	**+15.98%**
	8192	Verify	3596094	1741234	**+51.58%**
		Encrypt	3602484	1750415	**+51.41%**

References

[1] H. Becker, V. Hwang, M. J. Kannwischer, L. Panny, and B.-Y. Yang, "Efficient Multiplication of Somewhat Small Integers using Number-Theoretic Transforms," *IWSEC*, 2022.
[2] H. Becker et al., "Neon NTT: Faster Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1," *TCHES*, 2022(1), pp. 221–244.
[3] C.-M. Chiu, B.-Y. Yang, and B.-Y. Wang, "A New Trick for Polynomial Multiplication: A Verified CRT Polymul Utilizing a Monomial Factor," *TCHES*, 2025(4), pp. 795–816.
[4] T. Granlund and the GMP Development Team, *GNU MP 6.3.0 Manual: FFT Multiplication*, 2023.