Design of Flexible Processing Elements for NoC-Based NTT Accelerators

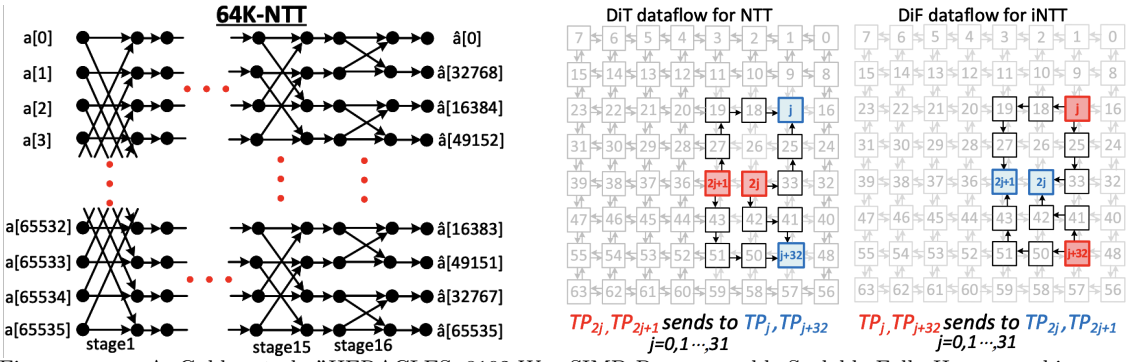


Figure source: A. Golder et al., "HERACLES: 8192-Way SIMD Programmable Scalable Fully-Homomorphic Encryption SoC for Privacy-Preserving Cloud Computing in Intel 3 CMOS," 2026 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, 2026, pp. 424-426.

Number Theoretic Transform (NTT) is a key building block for efficient polynomial multiplication in modern cryptographic systems, including fully homomorphic encryption (FHE), zero-knowledge proofs (ZKP), and post-quantum cryptography (PQC). As a result of its intensive modular arithmetic and memory access patterns, NTT is often the main computational bottleneck and is typically accelerated using dedicated hardware.

With the growing maturity of FHE, ZKP, and PQC schemes, hardware accelerators are increasingly moving from programmable platforms such as GPUs and FPGAs toward ASIC implementations. Recently, network-on-chip (NoC)-based architectures have emerged as a promising approach for scalable NTT acceleration (e.g., CHES'25 REED and ISSCC'26 HERACLES). However, the parameter sets of NTTs vary significantly across different cryptographic schemes and even across schemes within FHE. Consequently, many existing ASIC implementations either support only a limited class of primes or are optimized for a single fixed parameter set, which reduces flexibility.

This thesis focuses on exploring efficient and flexible ASIC front-end designs of NTT processing elements (PEs) for NoC-based NTT accelerators. The student will study the mathematical foundations of modular arithmetic and NTT algorithms, investigate low-level hardware implementations supporting multiple parameter sets, and explore the design space of flexible NTT architectures. The goal is to develop efficient NTT PEs that support diverse parameter sets while maintaining low area and power overhead.

Practicalities

Promotor:	Ingrid Verbauwhede		
Daily supervisor:	Zetao Miao	zetao.miao@esat.kuleuven.be	office 01.23
	Xander Pottier	xander.pottier@esat.kuleuven.be	office 01.21
Nature of the work:	15% literature, 15% writing, 70% modeling & implementation		
Number of students:	1		