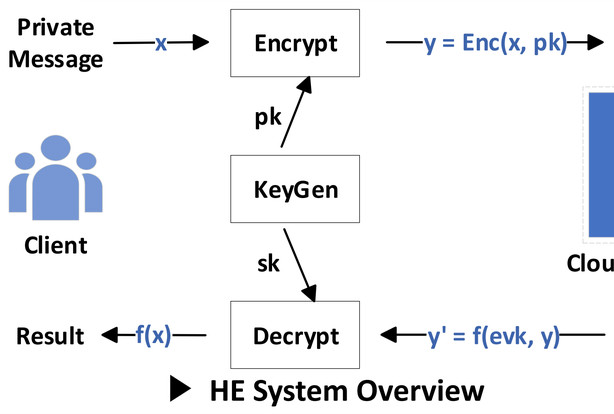
IDEC Chip Design Contest

An Energy-Efficient Number Theoretic Transform Accelerator for Fully Homomorphic Encryption

Sangouk Jeon, Dongsuk Jeon, Seoul National University, Seoul, Korea

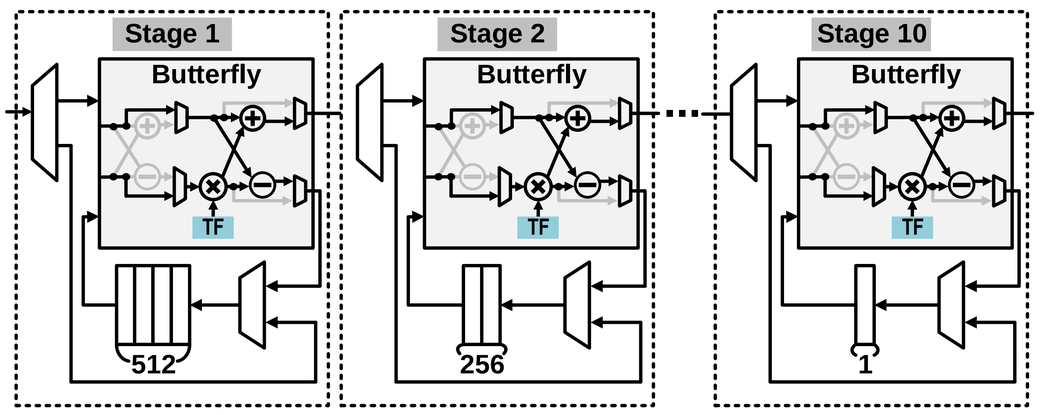
Motivation



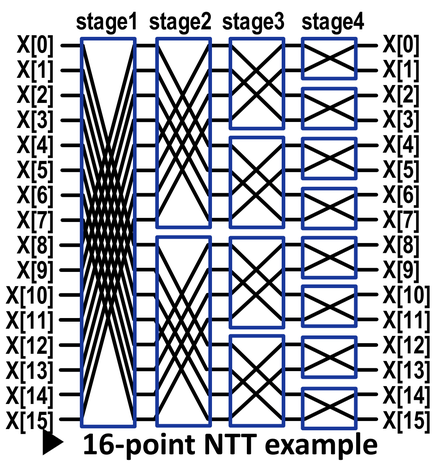
▶ HE System Overview

In HE System, Large-bit Computation → Area, Power Overhead ↑

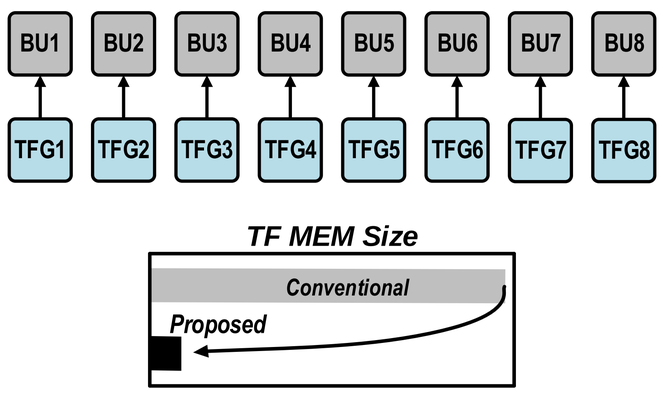
Number Theoretic Transform



▶ Pipelined NTT architecture (1024-NTT example)

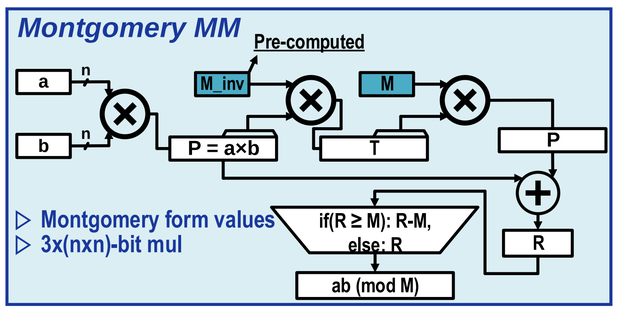


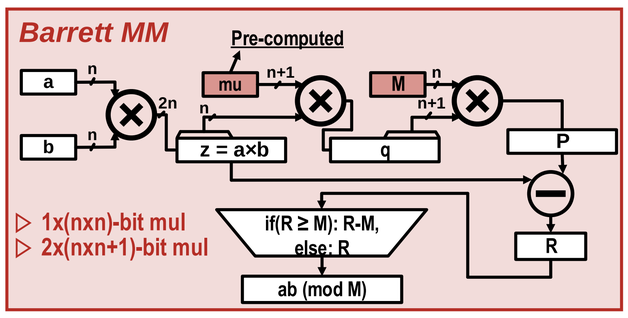
▶ 16-point NTT example



▶ Twiddle Factor Generation

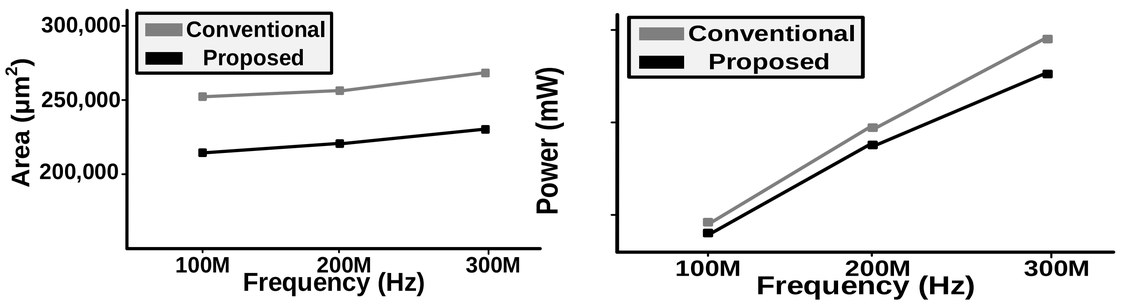
Proposed Modular Multiplier



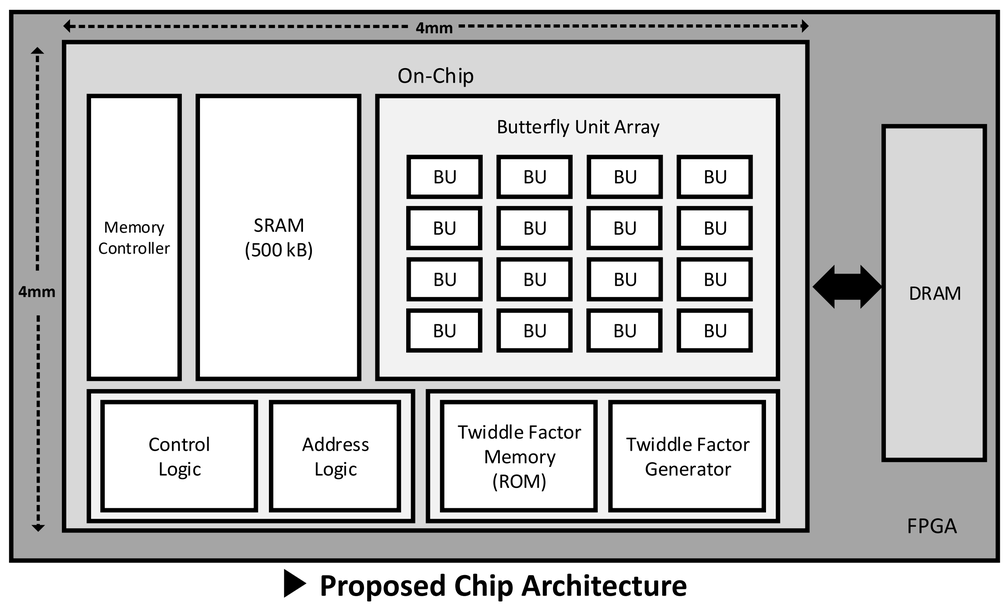


Conventional Montgomery & Barrett Modular Multiplication →3 x Large-bit multiplication needed

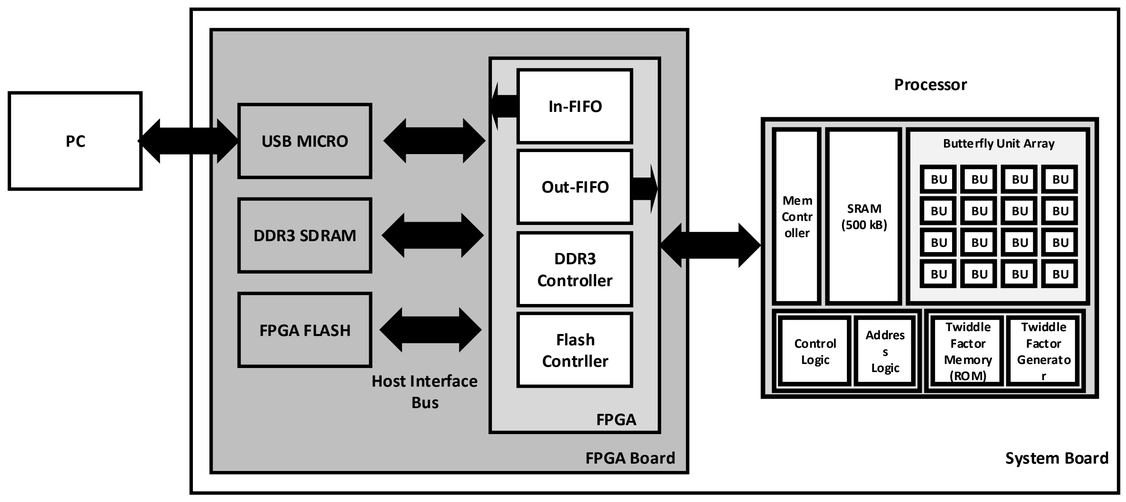
Proposed MM efficiently realizes the modular red uction algorithm.



Chip Architecture

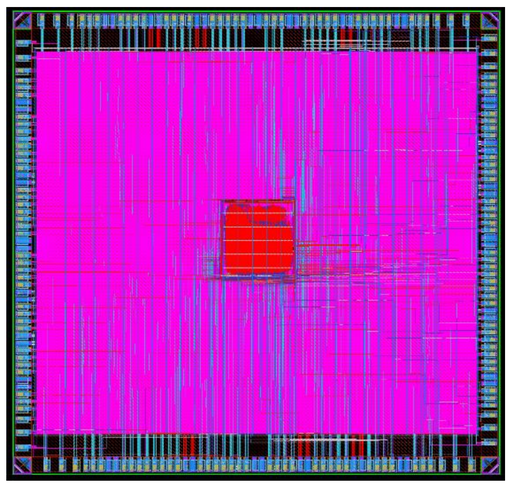


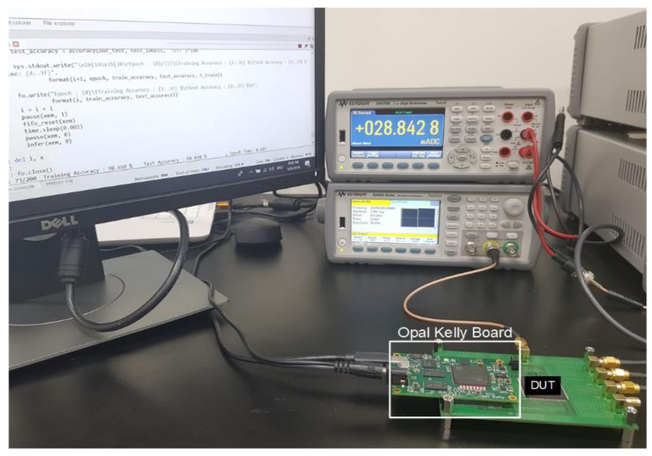
▶ Proposed Chip Architecture



▶ Verification system with proposed processor

Chip Layout & Measurement





▶ Layout of our design & Measurement setup using Opal kelly Board

Result & Conclusion

▶ Efficient modular multiplier that efficiently realizes the modular reduction algorithm.
▶ On-the-fly twiddle factor generation, reducing on-chip memory requirements.
▶ Pipelined NTT using a network of multiple butterfly units.
▶ Optimize dataflow for high data utilization.

The design was fully verified in simulations, but it still has some issues in measurements. We plan to continue measurements and try to identify and resolve the underlying issues.

[1] A. Q. A. Al Badawi, Y. Polyakov, K. M. M. Aung, B. Veeravalli, and K. Rohloff, "Implementation and performance evaluation of RNS variants of the BFV homomorphic encryption scheme," in IEEE Transactions on Emerging Topics in Com puting, vol. 9, no. 2, 2021.
[2] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," ACM Transactions on Computation Theory (TOCT), vol. 6, no. 3, 2014.
[3] Cheon JH, Kim A, Kim M, Song Y, "Homomorphic encryption for arithmetic of approximate numbers," in International Conference on the Theory and Application of Cryptology and Information Security, Dec 2017, pp. 409-437.'