Designed and integrated an efficient data bus.
Designed and integrated an efficient data bus.
Alternative approach

IDEC Chip Design Contest

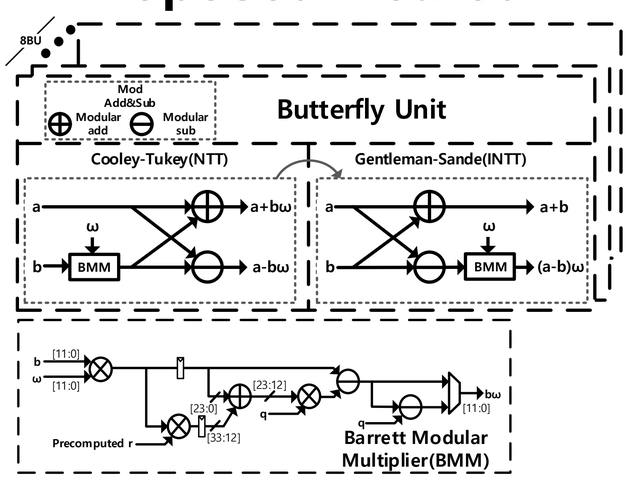
A Lattice-Based Cryptography Accelerator for Crystals-Kyber Algorithm

Jin Young Choi and Jongmin Lee
Department of Intelligence Semiconductor Engineering, Ajou University
jongmin@ajou.ac.kr

I. Intorduction

- CRYSTALS-Kyber
  - Adopted as a next-generation PQC algorithm.
  - Lattice based cryptography leveraging Module learning with Error(M-LWE) problem. (Matrix multiplication is required)

II. Proposed Method



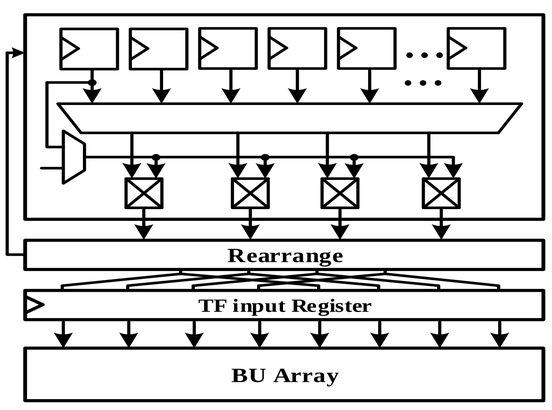


Fig.1 Proposed Butterfly Unit and Twiddle Factor Generator

- Barrett Modular Multiplication
  - Utilize specific bit ranges from intermediate results.
- Unified butterfly
  - Both Cooley-Tukey and Gentleman-Sande operations.
- Twiddle factor generator
  - Generates twiddle factors using minimal seed data.

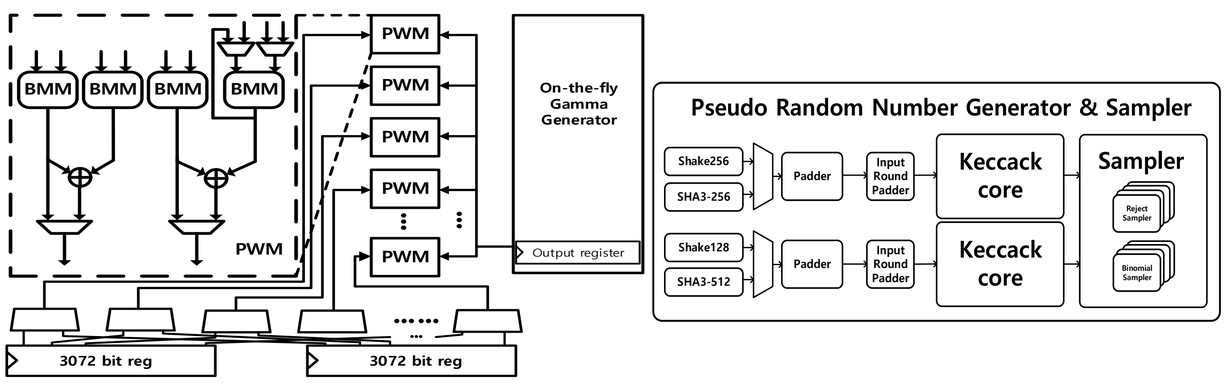
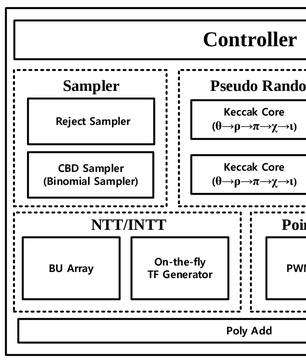


Fig.2 Proposed Point-wise multiplication and PRNG & Sampler

- Point-wise multiplication(PWM)
  - Feedback structure of Barrett modular multiplication.
  - On-the-fly Gamma generator
- PRNG and Sampler
  - Integrated two Keccak cores.
  - 24 clock cycle Keccak output. (θ→ρ→π→χ→ι)
  - Reject sampler and Centered binomial sampler



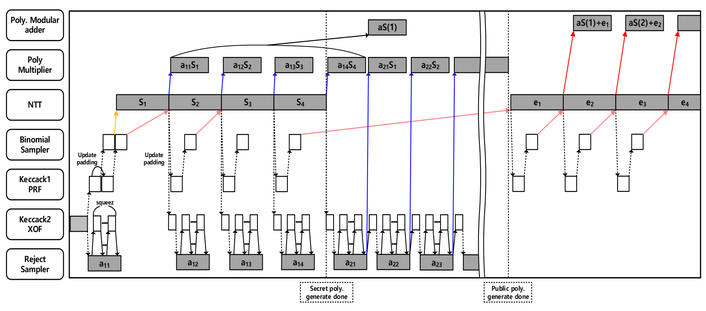


Fig.3 Top-level Architecture and Scheduling

- Top-level Architecture
  - Sampler, PRNG, NTT/INTT engine, PWM engine.
- Scheduling
  - Minimize the idle time of each module.
  - Efficiently performs matrix multiplication.

III. Result

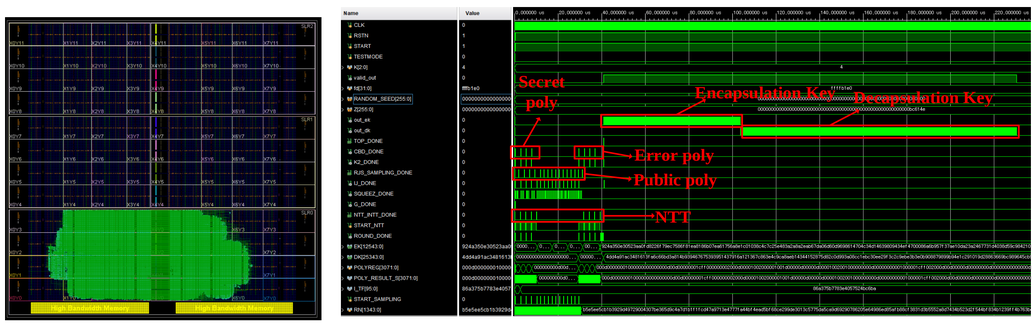


Fig.4 FPGA Implementation result and Simulation result

Work	ISSCC'15	CICC'18	ISSCC'19	Proposed
# of Twiddle Factor Seed	512	512	512	8
NTT Cycles	1700	160	1288	455
Sample Cycles (Binomial Sampler)	-	3704 (N=512)	1009 (N=512)	496 (N=256)
Sample Cycles (Reject Sampler)	-	-	-	474 (N=256)

Table1. Performance comparison

- Improved Plan
  - Integrate serial communication in submodules
  - Design and integrate efficient data bus
- Alternative
  - Implemented in FPGA platform (VCU-118)
  - Utilization (LUT/FF/DSP) = (184,575 / 127,719 / 144)
  - M-LWE Matrix size up to (k,l) = (4,4)
- Performance Comparison
  - # of Twiddle factor seed required reduced up to 98.4%
  - 455cc per NTT operation
  - 496cc per binomial sampling / 474 per reject sampling

IV. Conclusion

- Optimization of submodules
  - NTT, Barrett Modular Multiplication, Point-wise Multiplication, Twiddle Factor Generator, PRNG and Sampler.
- Efficient scheduling
  - Efficiently performs Matrix Multiplication ($a \cdot s+e$) and enhancing data throughput.