**Design of pipelined NTT-based polynomial multiplier for Post-Quantum Cryptography CRYSTALS-Kyber**

Abstract – In this paper, we present a high-speed and pipelined fully hardware polynomial multiplier design based on number theoretic transform (NTT). NIST post-quantum cryptography standardization round 3 announced CRYSTALS-Kyber as one of the finalists. As a lattice-based cryptography scheme, CRYSTALS-Kyber relies heavily on polynomial multiplication efficiency. Our work centers around designing and optimizing the polynomial multiplier architecture for accelerating hardware implementation of CRYSTALS-Kyber. This includes modifying the modular arithmetic modules, memory and data processing sequences. As a result, our designed achieved 231 MHz Fmax synthesized on Intel FPGA Cyclone V with Quartus, a 15% improvement in speed compared to similar work. Resources utilization through combinational logic path re-balance allowed us to efficiently pipelining between hardware modules.

1. Introduction

The National Institute of Standards and Technology (NIST) announced Post-Quantum Cryptography Standardization process since 2016 [1]. The goal of the standardization is to establish new cryptographic system for both classical computers and quantum computers in the future. Research and development progress in Post-Quantum Cryptography improved significantly through recent years. In 2020, third round candidates were announced, with 4 out of 5 finalists for Public-key Encryption and Key-establishment Algorithms are lattice-based cryptography scheme. Lattice-based cryptography, together with Learning with Errors problem (LWE), are proven to be safe-to-use under worst-case scenario and offer good trade-off between efficiency and security. CRYSTALS-Kyber is one of the five finalists in round 3.

CRYSTALS-Kyber is a lattice-based IND-CCA2-secure key-encapsulation mechanism (KEM), based on Module-LWE problem [2]. It also has a digital signature sibling, called CRYSTALS-Dilithium [3]. Kyber requires heavy computational effort, mostly as multiplication of polynomials over a constant-size polynomial ring. This scheme over “module lattices” offers good trade-off between efficiency and security. The key generation, encryption and decryption process however could account for a large proportion of computing power and clock cycles on microprocessors. Kyber describe a technique called Number Theoretic Transform (NTT), which reduce the complexity of polynomial multiplication from O(n2) to O(nlogn). While the scheme and technique could be parallel computed, the pure software implementation does not fully utilize the ability.

Many lattice-based cryptographical scheme are implemented on software as a proof of concept and utility, but the wide implementation of them is more likely to be processed on co-hardware and software or fully hardware solutions. Many PQCs candidates and projects have their research design on a FPGA, ASIC or co-processor for ARM, RISC V. One of the earliest full hardware implementations of PQC [3] is for Round5, this includes a hardware design of Keccak, AES-GCM and Round5 algorithm. The simplicity from Round5 modular advantages is used efficiently on hardware. In [4], a similar full hardware design of CRYSTALS-Kyber is presented, which speed-up the performance 129 times compare to Cortex-M4 processor implementation [5]. In [6], the first side-channel attack protected design of hardware CRYSTALS-Kyber is shown with impressive performance. Zhao et al. [7] analyze the software code to optimize their design, which yields positive results. Other implementation of Kyber varies from hardware and software processor hybrids [8] [9] [10] to pure hardware [5] [6] [11] [12]. More recent research on CRYSTALS-Kyber hardware implementation optimizes mostly on its polynomial multiplication process, which is also the purpose of our research. [13] present a novel modular technique called K2-RED for their NTT structure, which improve modular performance. A different modular technique is used in [14], modified with pre-computed constants. Zhang et al. [15] present a ping-pong memory access scheme to efficiently accessing the RAM. Our proposed design improves in modular reduction technique and resource efficiency compared to [13], [14], [15].

In this paper, we present a hardware NTT-based polynomial multiplier optimized for CRYSTALS-Kyber PQC scheme. The architecture includes a uniform NTT/Invert NTT butterfly unit with improved modular functions, pre-computed parameters and a dual memory accessing sequence which speed-up the computing process. The combinational circuit are pipelined down to 2 logic levels to maximize timing result, further increase the performance of the multiplier.

The rest of the paper is organized as followed. Section II explains the preliminaries for Number Theoretic Transform (NTT) and CRYSTALS-Kyber. In section III, we present the hardware design for Kyber NTT-based polynomial multiplier. We compare and discuss the synthesis and simulation result in section IV and concludes the paper in section V.

1. Preliminaries

In this section, we briefly describe CRYSTALS-Kyber scheme and related mathematical information.

1. CRYSTALS-Kyber scheme

CRYSTALS-Kyber is based on the module-lattice learning-with-errors problem (MLWE [16]). The detail

1. Kyber polynomial multiplication
2. The proposed design
3. The results
4. Conclusion
5. References.
6. [NIST: Post-Quantum Cryptography Standardization https://csrc.nist.gov/Projects/post-quantum-cryptography.](https://jlc.jst.go.jp/DN/JALC/00156214771?type=list&lang=ja&from=J-STAGE&dispptn=1)
7. Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, and Damien Stehlé. CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018. IEEE, 2018. To appear. https://eprint.iacr.org/2017/634. 4, 11, 23
8. Andrzejczak, Michal, Farnoud Farahmand, and Kris Gaj. "Full Hardware Implementation of the Post-Quantum Public-Key Cryptography Scheme Round5." *2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*. IEEE, 2019.
9. Huang, Yiming, et al. "A pure hardware implementation of crystals-kyber PQC algorithm through resource reuse." *IEICE Electronics Express* (2020): 17-20200234.
10. B. Leon, et al.: “Memory-efficient high-speed implementation of Kyber on Cortex-M4,” International Conference on Cryptology in Africa (2019) 209-228 (DOI: 10.1007/978-3-030-23696-0\_11)
11. Jati, Arpan, et al. "A Configurable Crystals-Kyber Hardware Implementation with Side-Channel Protection." *Cryptology ePrint Archive* (2021).
12. Zhao, Yixuan, et al. "Optimization Space Exploration of Hardware Design for CRYSTALS-KYBER." *2020 IEEE 29th Asian Test Symposium (ATS)*. IEEE, 2020.
13. Albrecht, Martin R., et al. "Implementing RLWE-based schemes using an RSA co-processor." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019): 169-208.
14. Sanal, Pakize, et al. "Kyber on ARM64: Compact Implementations of Kyber on 64-bit ARM Cortex-A Processors."
15. Seo, Hwa-jeong, et al. "Optimized implementation of scalable multi-precision multiplication method on RISC-V processor for high-speed computation of post-quantum cryptography." *Journal of the Korea Institute of Information Security & Cryptology* 31.3 (2021): 473-480.
16. Xing, Yufei, and Shuguo Li. "A compact hardware implementation of CCA-secure key exchange mechanism CRYSTALS-KYBER on FPGA." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021): 328-356.
17. Guo, Wenbo, Shuguo Li, and Liang Kong. "An Efficient Implementation of KYBER." *IEEE Transactions on Circuits and Systems II: Express Briefs* (2021).
18. Bisheh-Niasar, Mojtaba, Reza Azarderakhsh, and Mehran Mozaffari-Kermani. "High-Speed NTT-based Polynomial Multiplication Accelerator for CRYSTALS-Kyber Post-Quantum Cryptography." Cryptol. ePrint Arch., Tech. Rep 563 (2021): 2021.
19. Yarman, Ferhat, et al. "A hardware accelerator for polynomial multiplication operation of CRYSTALS-KYBER PQC scheme." *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2021.
20. Zhang, Cong, et al. "Towards Efficient Hardware Implementation of NTT for Kyber on FPGAs." *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2021.
21. Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 75(3):565–599, 2015. https://eprint.iacr.org/2012/090. 4, 12, 19