May 8, 2025

Lang Li
Email: lilang911@126.com
Hengyang, Hunan Province, China, 421002

Dear Editor,

The manuscript titled "Thread-Adaptive: Optimized Parallel Architectures of SLH-DSA on GPUs" is hereby submitted for consideration to *IEEE Transactions on Circuits and Systems Part II: Express Briefs*. All co-authors have thoroughly reviewed and approved this submission, and we confirm that this manuscript is not under consideration by any other publication.

Our work addresses a critical need in post-quantum cryptography by presenting a novel GPU-accelerated implementation of SLH-DSA (FIPS 205), employing thread-adaptive parallelization methodologies to significantly enhance throughput. The research makes three substantial contributions to the field of hardware-accelerated cryptography: (1) An innovative Adaptive Thread Allocation framework that dynamically optimizes thread configurations for specific cryptographic operations based on their computational profiles and resource requirements; (2) A sophisticated Function-Level Parallelism architecture that strategically decomposes cryptographic operations into independent computational tasks, enabling efficient GPU utilization across diverse parameter sets; (3) Comprehensive performance analysis demonstrating exceptional throughput improvements, with our implementation achieving 62,239 signatures per second for the SHA2-128f parameter set—a 1.16$\times$ improvement over the current state-of-the-art implementations.

This manuscript aligns perfectly with *IEEE Transactions on Circuits and Systems Part II: Express Briefs* as the premier venue for advanced hardware acceleration research. Our thread-adaptive architecture directly addresses the journal's areas of cryptographic hardware implementation (DCS120B0) and cryptography architectures (DCS120A5). While the journal has previously published related works on GPU-accelerated cryptography, such as Lee et al.'s AES implementations, our research extends the field in a novel direction by introducing adaptive parallelization strategies specifically optimized for post-quantum signature schemes—an approach particularly relevant given the increasing importance of quantum-resistant cryptography. The concise yet technically rich format of Express Briefs provides the ideal platform to showcase our focused methodological contribution. All code, data, and materials supporting our findings will be made available upon publication to facilitate reproducibility and further research.

Your time and consideration are greatly appreciated. Please do not hesitate to request any additional information or clarification.

Sincerely yours,

Lang Li
College of Computer Science and Engineering
Hengyang Normal University, China