Efficient Implementations of SPHINCS+ on GPUs

Jiahao Xiang and Lang Li.

***Abstract*—The Post-Quantum Cryptography (PQC) standardization process has led to the development of SPHINCS+, a stateless hash-based signature scheme that provides long-term security. The high computational cost of SPHINCS+ has motivated research into efficient implementations on various platforms. In this work, we present a GPU-based implementation of SPHINCS+ that achieves high throughput while maintaining security guarantees. Our implementation leverages the parallel processing capabilities of GPUs to accelerate the signature generation process. We evaluate the performance of our implementation on an NVIDIA RTX 4090 GPU and demonstrate that it can achieve a throughput of xxx for the SPHINCS+ signature generation. Our results show that GPUs can be an effective platform for accelerating SPHINCS+ and other post-quantum cryptographic schemes.**

***Index Terms*—Software implementation, GPU, signature algorithm.**

I. Introduction

THE quantum computers leverage quantum-mechanical phenomena to process data, raising significant concerns about the resilience of classical cryptographic methods. The security offered by widely deployed public-key cryptosystems, such as RSA and ECC, is jeopardized by Shor's algorithm [1], motivating comprehensive research on alternative cryptographic solutions. In response, the National Institute of Standards and Technology (NIST) initiated the Post-Quantum Cryptography (PQC) standardization process to develop novel schemes that withstand quantum computing capabilities [2].

SPHINCS+ is a representative stateless hash-based signature scheme and a finalist in the ongoing NIST standardization effort [3]. Long-term security against advanced quantum attacks is targeted by employing robust cryptographic hash functions [4]. The high computational cost of SPHINCS+ has motivated further investigations into efficient implementations across CPUs, FPGAs, and GPUs [5] to facilitate smooth adoption by organizations transitioning to post-quantum cryptography.

A. Related Work

Several prior studies have explored the efficient implementations of post-quantum signature schemes on various platforms. The work in [5] has provided initial investigations into GPU-based implementations. Additionally, CUSPX [6] has been introduced, demonstrating the first large-scale parallel implementation of SPHINCS+. CUSPX employs a three-level parallelism framework—integrating algorithmic, data, and hybrid strategies and introduces novel parallel Merkle tree construction algorithms combined with multiple load-balancing approaches. These contributions have significantly advanced the state-of-the-art in the efficient implementation of SPHINCS+.

This work is supported by the Hunan Provincial Natural Science Foundation of China (2022JJ30103), Postgraduate Scientific Research Innovation Project of Hunan Province (CX20240977), "the 14th Five-Year Plan" Key Disciplines and Application-oriented Special Disciplines of Hunan Province (Xiangjiaotong [2022] 351), the Science and Technology Innovation Program of Hunan Province (2016TP1020).

Jiahao Xiang and Lang Li are affiliated with the Hunan Provincial Key Laboratory of Intelligent Information Processing and Application, as well as the Hunan Engineering Research Center of Cyberspace Security Technology and Applications, both located at Hengyang Normal University, Hengyang 421002, China. They are also faculty members of the College of Computer Science and Technology at Hengyang Normal University. (e-mail: jiahaoxiang2000@gmail.com; lilang911@126.com)

B. Motivation

C. Contributions

II. Preliminaries

III. GPU-based Implementation of SPHINCS+

IV. Performance Evaluation

V. Conclusion

References

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[2] National Institute of Standards and Technology, "Report on post-quantum cryptography," National Institute of Standards and Technology, Tech. Rep. NISTIR 8105, 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[3] M. S. Turan, K. McKay, D. Chang, L. E. Bassham, J. Kang, N. D. Waller, J. M. Kelsey, and D. Hong, "Status report on the final round of the nist lightweight cryptography standardization process."

[4] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The sphincs+ signature framework," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*, L. Cavallaro, J. Kinder, X. Wang, and J. Katz, Eds. ACM, 2019, pp. 2129–2146.

[5] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nat.*, vol. 605, no. 7909, pp. 237–243, 2022.

[6] Z. Wang, X. Dong, H. Chen, Y. Kang, and Q. Wang, "Cuspx: Efficient gpu implementations of post-quantum signature sphincs¡sup¿+¡/sup¿," *IEEE Transactions on Computers*, vol. 74, no. 1, pp. 15–28, 2025.