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.**

I. Introduction

The Advanced Encryption Standard (AES) is a widely adopted symmetric block cipher that provides essential security in diverse communication protocols [1]. Commonly used libraries such as OpenSSL and Libgcrypt employ T-table-based methods for both encryption and decryption, delivering adequate performance for megabit-per-second workloads [2], [3].

Performance shortcomings arise when data rates exceed gigabit-per-second thresholds [4]. Such high-throughput scenarios, including data centers and 5G networks, require more efficient and scalable solutions to preserve both speed and cryptographic strength.

A. Related Work

The parallel structure of GPUs supports the simultaneous execution of multiple threads, which significantly increases performance in comparison with standard CPU-based operations. Table I summarizes representative AES CTR mode implementations on GPUs. In [5], the overhead of the ShiftRows stage is minimized by rearranging input data, and a hardware-based S-box replaces look-up table resources in the Substitute Bytes stage. In [6], the necessity to embed round keys at compile time is eliminated, allowing more flexible code generation. This approach achieves 9% higher encryption throughput than bit-sliced references for CTR modes.

TABLE I
Related Work on AES CTR mode Implementations on GPUs

Ref	Throughput (Gbps)	Platform	Year
[5]	1478	Tesla V100	2019
[6]	1489	RTX 3080	2022
Ours	–	RTX 4090	–

B. Motivation

C. Contributions

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 with the Hunan Provincial Key Laboratory of Intelligent Information Processing and Application, Hengyang Normal University, Hengyang 421002, China, and also with the College of Computer Science and Technology, Hengyang Normal University, Hengyang 421002, China (e-mail: jiahaoxiang2000@gmail.com; lilang911@126.com).

References

[1] J. Daemen and V. Rijmen, *The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition*, ser. Information Security and Cryptography. Springer, 2020.

[2] J. Jancar, M. Fourné, D. D. A. Braga, M. Sabt, P. Schwabe, G. Barthe, P. Fouque, and Y. Acar, "They're not that hard to mitigate: What cryptographic library developers think about timing attacks," in *Software Engineering 2024, Fachtagung des GI-Fachbereichs Softwaretechnik, Linz, Austria, February 26 - March 1, 2024*, ser. LNI, R. Rabiser, M. Wimmer, I. Groher, A. Wortmann, and B. Wiesmayr, Eds., vol. P-343. Gesellschaft für Informatik e.V., 2024, pp. 143–144.

[3] B. Marshall, G. R. Newell, D. Page, M. O. Saarinen, and C. Wolf, "The design of scalar AES instruction set extensions for RISC-V," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2021, no. 1, pp. 109–136, 2021.

[4] L. Li, J. Fang, J. Jiang, L. Gan, W. Zheng, H. Fu, and G. Yang, "Efficient AES implementation on sunway taihulight supercomputer: A systematic approach," *J. Parallel Distributed Comput.*, vol. 138, pp. 178–189, 2020.

[5] O. Hajihassani, S. K. Monfared, S. H. Khasteh, and S. Gorgin, "Fast AES implementation: A high-throughput bitsliced approach," *IEEE Trans. Parallel Distributed Syst.*, vol. 30, no. 10, pp. 2211–2222, 2019.

[6] W.-K. Lee, H. J. Seo, S. C. Seo, and S. O. Hwang, "Efficient implementation of aes-ctr and aes-ecb on gpus with applications for high-speed frodokem and exhaustive key search," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, pp. 2962–2966, 2022.

Jiahao Xiang is pursuing a Master's degree in Electronic Information at Hengyang Normal University, China. His research focuses on cryptographic engineering and efficient implementations of block ciphers on resource-constrained devices. Publications include works on lightweight cryptography optimization and contributions to open-source cryptographic projects.

Lang Li received his Ph.D. and Master's degrees in computer science from Hunan University, Changsha, China, in 2010 and 2006, respectively, and earned his B.S. degree in circuits and systems from Hunan Normal University in 1996. Since 2011, he has been working as a professor in the College of Computer Science and Technology at the Hengyang Normal University, Hengyang, China. He has research interests in embedded system and information security.