High Throughput Implementation of AES on GPUs

Jiahao Xiang and Lang Li.

***Abstract*—The rapid increase in data transfer rates from gigabits per second to terabits per second necessitates efficient computational approaches for high-speed data processing. Traditional software and extended instruction set architectures prove inadequate under these conditions. A GPU-based software implementation of the AES is presented, employing bitslicing to compute substitutions on the fly and thereby reducing cache misses compared with look-up table methods. Additional gains are realized through a permutation optimization that mitigates thread stall time. Experimental results indicate that this implementation achieves throughput in xx.xx terabit-per-second when executed on a single NVIDIA RTX 4090 GPU.**

***Index Terms*—Software implementation, Block cipher, GPU, Bitslicing, SAT.**

I. Introduction

THE Advanced Encryption Standard (AES) is recognized as a widely adopted symmetric block cipher that underpins secure communication protocols [1]. Libraries such as OpenSSL and Libgcrypt rely on T-table-based methods for both encryption and decryption, providing sufficient performance for megabit-per-second (Mbps) workloads [2], [3].

However, T-table approaches have been shown to be inadequate when data rates reach gigabit-per-second (Gbps) or terabit-per-second (Tbps) ranges [4]. These higher-speed environments, including data centers, 5G networks, and real-time transactional systems, necessitate more efficient and scalable techniques to maintain throughput while preserving cryptographic security.

A. Motivation

B. Related Work

[5]

C. Contributions

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] 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.

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).

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.