TESLAC: Accelerating Lattice-based Cryptography with AI Accelerator ⋆

Lipeng Wan[1,2,3], Fangyu Zheng[1,3(✉)], and Jingqiang Lin[3]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[3] Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing, China
[4] School of Cyber security, University of Science and Technology of China

Abstract. In this paper, we have brought AI accelerator to implement cryptographic algorithms. To the best of our knowledge, it is the first attempt to implement quantum-safe Lattice-Based Cryptography (LBC) with AI accelerator. However, AI accelerators are designed for machine learning workloads (e.g., convolution operation), and cannot directly deliver their strong power into the cryptographic computation. On the other hand, polynomial multiplication over rings is a kind of time-consuming computation in LBC. To this end, we utilize a straightforward approach to make the AI accelerator fit well for polynomial multiplication over rings. Additional non-trivial optimizations are also made to minimize the overhead of transformation, such as using low-latency shared memory, coalescing memory access. Moreover, based on NVIDIA AI accelerator, Tensor Core, we have implemented a prototype system named TESLAC and give a set of comprehensive experiments to evaluate its performance. The experimental results show TESLAC can reach tens of millions of operations per second, achieving a performance speedup of two orders of magnitude from the AVX2-accelerated reference implementation. Particularly, with some techniques, TESLAC can also be scaled to other LBC with larger modulo q.

Keywords: Lattice-based Cryptosystems · Polynomial Multiplication Over Rings · AI Accelerator · Tensor Core · LAC

1 Introduction

Quantum computing has brought a huge security challenge to the widely-used conventional cryptosystems. If large-scale quantum computers are ever built,

⋆ This work was partially supported by National Key R&D Program of China under Award 2018YFB0804401 and National Natural Science Foundation of China under Award No. 61902392. *(Corresponding author: Fangyu Zheng, E-mail: zhengfangyu@iie.ac.cn).*