Bachelor-Thesis

GPU Implementation of BigInt Multiplication for the Post-Quantum Key Exchange Scheme SIKE

Institute for Scientific Computing

SCIENTIFIC COMPUTING

Giang Nam Nguyen, M.Sc.
Contact person

Alexanderstr. 2
64289 Darmstadt

Phone: +49 6151 16 - 27287
Fax: +49 6151 16 - 25345

giang_nam.nguyen@tu-darmstadt.de

https://www.sc.informatik.tu-darmstadt.de/

Date
October 9, 2020

While practical applications of quantum computers are not expected in the near future, over the last two decades, the cryptography research community is moving towards post-quantum schemes.

Isogeny-based cryptography attracts many research interest. It is originated from the idea of Jao et al. in [1] to build a Diffie-Hellman-like encryption scheme based on the hardness of the Computational Supersingular Isogeny Problem (CSSI). In practice, an isogeny-based key exchange scheme named SIKE was accepted as a candidate in the third round of the standardization process for post-quantum cryptography called by the U.S. National Institute of Standards and Technology (NIST).[1]

The arithmetic for BigInt, especially the multiplication operation, is a big concern to achieve an efficient implementation of SIKE. Given a wide variety of existing high-performance libraries, e.g. the CUDA toolkit[2], NVIDIA GPUs are the architecture of interest to speed up this calculation.

The goals of this thesis are:

- to implement the BigInt multiplication on GPUs by using the Fast Fourier Transformation on GPUs, e.g. see [2, 3],
- to assess the GPU implementation's performance, taking into account different data layouts for storing the BigInt,
- to compare its performance with that of the existing optimized CPU implementation.[3]

Recommendations

- Basic knowledge about post-quantum cryptography.
- Good programming skills in C/C++ and CUDA.
- The student is encouraged to write this thesis in English.

[1] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[2] Hovhannes Bantikyan. Big integer multiplication with cuda fft (cufft) library. *International Journal of Innovative Research in Computer and Communication Engineering*, 2(11):6317–6325, 2014.

[3] Jitendra V. Tembhurne. Parallel multiplication of big integer on gpu. In Pushpak Bhattacharyya, Hanumat G. Sastry, Venkatadri Marriboyina, and Rashmi Sharma, editors, *Smart and Innovative Trends in Next Generation Computing Technologies*, pages 276–285, Singapore, 2018. Springer Singapore.

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions
[2] https://docs.nvidia.com/cuda/cufft/index.html
[3] https://github.com/microsoft/PQCrypto-SIDH