Student-Assistant (HiWi) Job
HPC Solutions to Post-Quantum Crypto Schemes

TECHNISCHE UNIVERSITÄT DARMSTADT

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
March 19, 2021

The need for quantum-resistant cryptosystems arose from the fact that the quantum supremacy, which is demonstrated by the well-known Shor algorithm [1] for factorization, can be destructively used to break the current public key system like RSA or ECDSA.

Being involved as a research project within CROSSING, our research focuses on:

- **Lattice-based blind signature schemes.** In this context, we mainly focus on two schemes *blaze* and *blazePlus* [2]. The primary task is to refactor an existing C/C++ implementation of blazePlus in terms of adapting new parameters. Other schemes, which are being developed and share common building blocks with blazePlus, need also to be implemented. Upon achieving working implementations, another task is to optimize them on current CPU architectures.

- **Cryptanalysis in isogeny-based cryptography.** The hard problem which underlies this type of PQC is the CSSI problem [3]. The goal is to achieve a parallel solver utilizing GPUs as accelerators for compute-intensive parts of the algorithm. Thus, you will be involved in the development of a solver primarily targeting the host side (CPU). Furthermore, another task is to implement the isogeny computation, which is the hotspot of the solver, by employing the existing libraries for multi-precision integer arithmetic on GPUs.[1]

Requirements

- Successfully passed the course *Computersystemsicherheit*.[2]
- Good programming skills in C/C++.
- English for reading literature and writing documentation.

Working time

The working time may vary between 40-60 hours per month.

Contact

By interest, please send a short CV and the Transcript of Records to the Contact person.

[1] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, Oct 1997.

[2] Nabil Alkeilani Alkadri, Rachid El Bansarkhani, and Johannes Buchmann. On lattice-based interactive protocols: An approach with less or no aborts. Cryptology ePrint Archive, Report 2020/007, 2020. `https://eprint.iacr.org/2020/007`.

[3] Craig Costello, Patrick Longa, Michael Naehrig, Joost Renes, and Fernando Virdia. Improved classical cryptanalysis of sike in practice. Cryptology ePrint Archive, Report 2019/298, 2019. `https://eprint.iacr.org/2019/298`.

[1] Example: nvidia XMP 2.0 (https://github.com/NVlabs/CGBN)
[2] Enrollment in the course *Introduction to Cryptography* or *Post Quantum Cryptography* is recommended.