TECHNISCHE UNIVERSITÄT DARMSTADT

Master Thesis

Implementation of Post-Quantum Security Frameworks

1. General Information

Lattice-based cryptography is a very promising candidate for the future in case large-scale quantum computers are built. From hard computational assumptions based on lattices advanced primitives like homomorphic encryption and multi-party computation protocols (MPC) can be realized.
The objective of this thesis is to implement a complete post-quantum security application/framework including a graphical user interface.

2. Tasks

- Literature research
- Implementation of a security framework
- Implementation of a graphical user interface

3. Required Skills

The required skills, in order of importance, are:

- Very good knowledge in (lattice-based) cryptography.
- Good mathematical skills.
- Strong programming skills in Java
- Experience in the design of graphical user interfaces

Knowledge of the English language is required to get along with the technical literature.

4. Contact

If you are interested, please contact
Dr. Rachid El Bansarkhani
Room: S2|02 B212
EMail: elbansarkhani@cdc.informatik.tu-darmstadt.de

01.12.2017