TECHNISCHE UNIVERSITÄT DARMSTADT

The QPC group (Quantum and Physical attack resistant Cryptography) is offering a

Hiwi position

on the topic

Physical attacks on post-quantum cryptography.

Background & Task

When cryptography is used in practice, it is not sufficient that the schemes used fulfill theoretical security notions. They also have to be protected against physical attacks, i.e., side channel and fault attacks.
In the field of post-quantum cryptography, research on physical attack security started only a few years ago, hence new publications are constantly published.

The task is to provide an **overview of publications on physical attacks on post-quantum cryptography**, and to update it continuously. Thus, it is a literature research through which deep knowledge on post-quantum cryptography will be gained.

If case of interest, there are many master thesis topics which can arise from this work.

Requirements

- good knowledge in crypto, especially post-quantum crypto
- good knowledge of the English language
- ability to work independently
- experience with reading research papers is beneficial

- ideally also Ubuntu expertise to occasionally provide admin-support

Position

- Available immediately
- Duration: at least 3 months (may be extended, long-term cooperation is desirable)
- Workload: 10h per week (open to negotiation)

If you are interested, please get in touch and send your application (including a CV and transcript of records) to Dr. Juliane Krämer (juliane@qpc.tu-darmstadt.de).