



TECHNISCHE
UNIVERSITÄT
DARMSTADT

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

Hiwi position

on the topic

Runtimes and memory/storage requirements of cryptographic schemes.

Background & Task

The goal of this work is to create an **overview of runtimes and memory/storage requirements of classical and post-quantum cryptographic schemes**. The schemes will be compared regarding both theoretical analysis and practical evaluation, i.e., with respect to concrete implementations on different platforms and based on different programming languages.

The overview shall be done exclusively based on publications, programming projects of third parties, etc. There is no programming involved.

Requirements

- course Einführung in die Kryptographie
 - course Post-Quantum-Kryptographie
 - good understanding of programming
 - good knowledge of the English language
 - ability to work independently
- ideally also Ubuntu expertise to occasionally provide admin-support

Position

- Available immediately
- Duration: at least 3 months (may be extended)
- 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).