



Job ID: JR0047253

Job Category: Intern/Student

Primary Location: Nuremberg, DE

Other Locations:

Job Type: Intern

Master Thesis in Applied Cryptography – Applied Post Quantum Cryptography for Slim Modem Platforms (f/m)

Job Description

A candidate for a temporary position who has not yet graduated and is working towards a relevant technical Master's degree from a relevant academic institute.

The goal of this master thesis is to identify which PQC schemes are applicable to which use case of cryptography in Intel slim modem products, to compare suitable schemes with regard to different Key Performance Indicators KPIs and to describe how the schemes can be applied to and integrated into the Intel slim modem platform security architecture and the related production flows.

Steps to be taken during this project include:

- Understand which cryptographic schemes are used in Intel slim modem products, the corresponding use cases and the functional and security requirements on the underlying cryptographic schemes.
- Analyze which of the cryptographic schemes currently used in Intel slim modem products are vulnerable to attacks based on quantum computers.
- Analyze the state of the art of Post Quantum Cryptography PQC with regard to its applicability to the use cases and requirements identified earlier.
- Describe how PQC schemes can be applied and if necessary adapted to the Intel slim modem platform security architecture and production flow use cases.
- Compare suitable PQC schemes with regard to different key performance indicators KPIs, such as performance, security properties and practicability of key management.
- Identify gaps between the state of the art of PQC and the slim modem use cases and their requirements, i.e. identify those use cases and requirements for which no suitable PQC scheme is available yet.

Qualifications

- Studies in computer science or similar background almost finished all exams passed
- Good knowledge in applied cryptography and/or post quantum cryptography
- Good knowledge in information and communications security-Good English language skills
- Good analytical capabilities and readiness to work in a team

Inside this Business Group

The Mobile and Communications Group delivers the next generation of smartphones, tablets, feature phones, and connected devices with leading-edge technologies. MCG is chartered with providing optimal hardware, software, and connectivity ingredients for mobile devices and complete system solutions that deliver compelling user experiences and delight both consumers and business professionals.

Apply now:

[http://jobs.intel.com/ShowJob/Id/1442225/Master-Thesis-in-Applied-Cryptography-%E2%80%93-Applied-Post-Quantum-Cryptography-for-Slim-Modem-Platforms-\(f-m\)/](http://jobs.intel.com/ShowJob/Id/1442225/Master-Thesis-in-Applied-Cryptography-%E2%80%93-Applied-Post-Quantum-Cryptography-for-Slim-Modem-Platforms-(f-m)/)