Master Thesis - Specification of Algorithm Parameters for Post-quantum Cryptography

Motivation

- A strong quantum computer can break all cryptosystems that are used today in the internet. However, there are cryptographic algorithms, called post-quantum, that are secure against a quantum computer. These algorithms are not widespread and their standardization has just started. A significant part of this process is the specification of the format of the cryptographic keys and operations.

Goals

- Goal of this thesis is to create a specification for post-quantum cryptographic algorithms like Classic McEliece or Sphincs+. This specification is used to promote interoperability. This specification is then implemented in the Java programming language.

Tasks

- Specification of the format of the cryptographic algorithms and their properties.
- Design of the software.
- Implementation of the designed software in Java.
- Creation of test vectors for interoperability purposes.

Prerequisites

- Good knowledge in IT-security and cryptography.
- Good knowledge of Software-Design.
- Very good knowledge of Java.
- Thesis language can be English or German.

Literature


Start: Right away or by arrangement