h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

CRISP
National Research Center
for Applied Cybersecurity

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

- [NIST] https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

Start: Right away or by arrangement

The **User-Centered Security** (UCS) Research Group investigates how to design, build and evaluate usable and secure interactive and collaborative software and IT-systems that people will trust, based on established or novel IT-Security and HCI principles and mechanisms.

The Group is affiliated with CRISP, the National Research Center for Applied Cybersecurity.

Interested? Please contact us via email or personal.

Contact
Prof. Dr. Andreas Heinemann
andreas.heinemann@h-da.de

Alexander Zeier, M. Sc.
alexander.zeier@h-da.de

Website
https://ucs.fbi.h-da.de

Schöfferstr. 10
64285 Darmstadt

UCS
USER-CENTERED SECURITY
DARMSTADT ∞ BERLIN