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

CRISP
National Research Center
for Applied Cybersecurity

Master Thesis - Design and Implementation of a Testbed 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 implementation and integration into applications has just started. Developers of the algorithms and applications currently do not have lots of tools to check their implementation for correctness or interoperability.

Goals

- Goal of this thesis is to design and implement a testbed. This testbed can be used by designers and developers of post-quantum cryptographic libraries and/or applications to check interoperability and correctness.

Tasks

- Design of the software.
- Implementation of the designed software in Java.
- Design of a usable graphical user interface.
- Creation of test vectors for interoperability purposes.

Prerequisites

- Good knowledge of Software-Design.
- Very good knowledge of Java.
- Interest and basic knowledge in IT-security and cryptography.
- 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