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

ATHENE
National Research Center
for Applied Cybersecurity

Master Thesis or R&D study: Extension of GPU-accelerated PQC algorithms with comparison to alternative hardware accelerations

Motivation

As the computing power of quantum computers continues to increase, it is conceivable that mathematical problems such as integer factorization and the discrete logarithm problem can be solved in polynomial time using Shor's algorithm. Such a development could result in established cryptographic methods such as RSA and Diffie-Hellman being broken. For this reason, cryptographic methods that are resistant to quantum computers are becoming increasingly important. They are being actively researched and standardized. An indispensable topic here is the performance of PQC algorithms. A wide variety of variants are being developed, some of which are achieved via hardware acceleration.

Goal

The aim of this work is to build on an existing implementation in which GPU accelerated PQC algorithms were tested. The original implementation dealt with GPU accelerated PQC algorithms in one batch mode variant each. This is now to be expanded to include a single-mode variant. Furthermore, the GPU implementations created are to be compared with alternative hardware-accelerated PQC algorithms.

Tasks

- Research and Documentation of related Work regarding performance and ressource usage of PQC-Schemes
- Extension of an implementation on a test suite on the HDA GPU cluster
- Evaluation and comparison of the results
- Comparison with researched alternative hardware acceleration

Prerequisites

- Experience in C/C++ and with Linux
- Interest in low-level/hardware development.
- Interest and basic knowledge in IT-security and cryptography.
- Thesis language can be English or German.

Start:

- 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 **Applied Cyber Security Darmstadt** (ACSD) Research Group specializes in protection of IT-systems and applications. Our solutions include, based on the use case, aspects such as long-termness, provability or methods of offensive security (White Hacking).

Contact

Prof. Dr. Alexander Wiesmaier
alexander.wiesmaier@h-da.de

Gero Knoblauch, M. Sc.
gero.knoblauch@h-da.de

Websites
https://ucs.h-da.io
https://acsd.h-da.de

Office
Schöfferstr. 10
64287 Darmstadt

UCS
USER-CENTERED SECURITY
DARMSTADT ∞ BERLIN

acsd applied cyber security darmstadt