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

ATHENE
National Research Center for Applied Cybersecurity

Masterarbeit oder F&E Studie: Erweiterung GPU-Beschleunigter PQC-Algorithmen mit Vergleich zu alternativen Hardware-Beschleunigungen

Motivation

Im Zuge der fortwährenden Steigerung der Rechenleistung von Quantencomputern ist es denkbar, dass mathematische Probleme wie die Integer-Faktorisierung und das diskrete Logarithmus-Problem mittels Shors Algorithmus in polynomieller Zeit gelöst werden können. Eine solche Entwicklung könnte zur Folge haben, dass etablierte kryptografische Verfahren wie RSA und Diffie-Hellman gebrochen werden können. Deshalb gewinnen kryptografische Verfahren, die gegen Quantencomputer resistent sind, zunehmend an Bedeutung. Sie werden aktiv erforscht und standardisiert. Ein wichtiges Thema hierbei ist die Performance von PQC-Algorithmen. Hierbei werden interschiedlichste Varianten entwickelt, die teilweise über Hardwarebeschleunigung erreicht werden.

Ziel

Ziel dieser Arbeit ist es, auf einer bestehenden Implementierung, in der GPU beschleunigte PQC-Algorithmen getestet wurden, aufzubauen. Die ursprüngliche Implementierung beschäftigte sich mit GPU beschleunigten PQC-Algorithmen in jeweils einer Batch-Mode Variante. Diese soll nun, um jeweils eine Single-Mode Variante erweitert werden. Weiterhin sollen die erstellten GPU-Implementierungen mit alternativen Hardware-Beschleunigten PQC-Algorithmen verglichen werden.

Aufgaben

- Recherche und Dokumentation von verwandten Arbeiten bezüglich Performance und Ressourcenverbrauch von PQC-Schemes
- Erweiterung einer Implementierung auf einer Test-Suite auf dem HDA-GPU-Cluster
- Auswertung und Vergleich der Ergebnisse
- Vergleich mit recherchierter alternativer Hardwarebeschleunigung

Voraussetzungen

- Sicherer Umgang mit C/C++ und Linux.
- Interesse an low-level bzw. Hardware-naher Entwicklung.
- Interesse und Grundkenntnisse in IT-Security und Kryptografie
- Thesissprache kann sowohl Englisch als auch Deutsch sein.

Start:

- Nach Absprache

Die **User-Centered Security** (UCS) Forschungsgruppe untersucht das Design, die Entwicklung und evaluiert benutzbare, vertrauenswürdige, sichere, interaktive und kollaborative Software und IT-Systeme, basierend auf etablierte oder moderne IT-Sicherheit und HCI Prinzipien und Mechanismen.

Die **Applied Cyber Security Darmstadt** (ACSD) Forschungsgruppe ist auf den Schutz von IT-Systemen und Anwendungen spezialisiert. Unsere Lösungen beinhalten Aspekte, je nach Anwendungsfall, wie Haltbarkeit, Belegbarkeit, oder Methoden der offensiven Sicherheit (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