Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Master Thesis

Speeding-up Post-Quantum Cryptography on an RSA Co-Processor

Motivation

Recent advances in the field of quantum computers threaten our public key cryptography. A large enough quantum computer can easily break RSA and elliptic curve cryptography. Lattice-based cryptography has been selected by the US National Institute for Standards and Technology as a replacement. The polynomial arithmetic within lattices can be challenging to implement on constrained IoT devices. Therefore, researchers put effort into re-using cryptographic RSA accelerators for lattice-based cryptography.

Task Description

The goal of this thesis is to evaluate one or more mathematical mappings of polynomials defined over rings to big integers in a finite field. Recent work on this can be found in papers by Albrecht et al.[1] and Bos et al.[2]. The target platform is Google's open source processor OpenTitan[3] and its big number accelerator OTBN. Within this thesis the student evaluates different algorithms for polynomial multiplication regarding their performance and memory overhead.

Requirements

- Familiar with embedded systems programming: C or Rust
- Familiar with assembly programming
- Motivation to work with post quantum cryptography and its mathematical representations
- Motivation to work with cryptographic co-processors

Kontakt

Felix Oberhansl
Telefon: +49 89 322-9986-156
E-Mail: felix.oberhansl@aisec.fraunhofer.de

Tobias Stelzer
Telefon: +49 89 322-9986-0916
E-Mail: tobias.stelzer@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Hardware Security Department
Lichtenbergstraße 11, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de

[1] https://doi.org/10.13154/tches.v2019.i1.169-208
[2] https://eprint.iacr.org/2020/1303
[3] https://github.com/lowRISC/opentitan