Master's Thesis

Error Resilience in the Number-Theoretic Transform – PQC acceleration for safety-critical applications
Asymmetric cryptography is a core component of modern communication infrastructure. The existence of a sufficiently large quantum computer threatens all algorithms currently in use and recent developments in this field motivate the field of post-quantum cryptography (PQC), with the primary objective of developing secure and futureproof alternatives. To consolidate these efforts, the National Institute of Standards and Technology (NIST) is conducting a competition with the goal of selecting and standardizing the best available candidates.

In July 2022 four algorithms were selected, one Public-key Encryption and Key-establishment Algorithms (KEM) and three Digital Signature Algorithms (DSA). Of these four algorithms, three (including the two recommended for general purpose applications) are from the class of lattice-based schemes, i.e., they rely on difficult problems over lattices for their security.

The lattices in these schemes are represented by elements from a polynomial ring and arithmetic over this ring therefore plays a crucial role in their execution. To accelerate this arithmetic and, specifically, the multiplication of polynomials, the number-theoretic transform (NTT) is used. This approach is a generalization of the multiplication algorithms based on the fast Fourier transform (FFT), that have been long established in fields like signal processing. Since a considerable part of the computational complexity of these algorithms lies in this NTT, it is a prime candidate for HW acceleration and many works in literature have proposed such accelerators.

While considerable efforts have been made to offer fast and lean NTT accelerators, the topic of fault resilience has received little attention so far. In safety critical applications, as common in automotive or industrial fields, this resilience is an important feature and needs to be provided by the HW. On the other hand, these fields are traditionally price sensitive, so the additional chip area required for these features should be minimal. However, current approaches, such as those introduced by Sarker et al. [1], impose a large area (or latency) overhead.

The goal of this thesis is to address this shortcoming. First, the approaches published in literature shall be evaluated with regard to the relevant performance figures (area overhead, latency, …). Then, new approaches for error resilience in NTT calculation shall be developed, either based on improving upon existing methods or by adapting methods for error resilience in the computation of FFTs.

References


Prerequisites

Basic understanding of HW design

Good knowledge of algebra

Contact

georg.maringer@tum.de

Advisors

Georg Maringer
Lukas Holzbaur, Alexander Zeh (Infineon Technologies)