First-Order Masked Kyber on ARM Cortex-M4

Daniel Heinz[1],
Matthias J. Kannwischer[2], Georg Land[3], Peter Schwabe[2] and Daan Sprenkels[4]

[1] Research Institute CODE, Universität der Bundeswehr München, Germany
[2] Max Planck Institute for Security and Privacy, Bochum, Germany
[3] Ruhr-Universität Bochum, Germany
[4] Digital Security Group, Radboud University, Nijmegen, The Netherlands

Abstract. In this work, we present a fast and first-order secure Kyber implementation optimized for ARM Cortex-M4. The ongoing progress of the NIST standardization process for post-quantum cryptography and several presented side-channel attacks have raised an increased demand for side-channel analysis and countermeasures for the proposed finalists. On the foundation of the commonly used PQM4 project, we make use of previous optimizations for Kyber on a Cortex-M4. We further combine different ideas from various recent works on masking Saber and Kyber to achieve a better performance and improve the security in comparison to the original implementations. We show our performance results for first-order secure implementations. Our masked Kyber decapsulation on the ARM Cortex-M4 requires only 4,077,819 cycles which already includes randomness generation from the internal RNG. The masked key generation requires 2,735,925 cycles. We then practically verify our implementation by using the t-test methodology with 100,000 traces.

Keywords: Lattice-Based Cryptography · Kyber · Side-Channel Analysis · ARM Cortex-M4