Side-Channel Leakage Tests for Post-Quantum Crypto Modules

Markku-Juhani O. Saarinen
PQShield Ltd, Oxford, UK

Abstract

I'll describe side-channel tests for Post-Quantum Cryptography key encapsulation mechanisms (KEMs) and stateful/stateless signature algorithms. The focus is on lattice-based NIST finalists. This work aims at developing types of tests that may be considered to become a part of the FIPS certification process for PQC algorithms. Hence the methodology aligns with the "push-button" TVLA (Test Vector Leakage Assessment) approach of the latest versions of ISO/IEC 17825, which is being adopted for FIPS 140-3 at levels 3-4. The tests allow one to assess the coverage of countermeasures against attacks based on power, electromagnetic emissions, and timing channels.

We describe algorithm-dependent (but implementation-neutral) test vectors and analysis methods designed to expose Critical Security Parameter (CSP) leakage in PQC algorithms. The tests are repeatable, but consistent trace acquisition and improved test calibration are essential. There are shortcomings as well: Leakage detection tests can't fully replace more time-consuming manual penetration testing and analysis of "attack potential." Furthermore, if not correctly interpreted, there is a risk of false positives (detection of non-CSP leakage).

Black-box tests of this type are already in industrial use as they allow third parties to verify the coverage of side-channel countermeasures independently, in a semi-automatic fashion. I will show some results of these tests against real-life hardware PQC modules.

Dr. Markku-Juhani O. Saarinen is a Senior Cryptography Architect at PQShield in Oxford, UK. He designs post-quantum cryptography IP and coprocessors. Markku has over 25 years of experience in cryptography and security engineering. He is best known for his research and standardization work with cryptographic protocols, post-quantum cryptography, random numbers, and implementation / side-channel security. Recent public contributions include the RISC-V Entropy Source extension and the RISC-V Data-Independent Latency (constant-time) instruction set. He holds a Ph.D. in Information Security (cryptanalysis) from Royal Holloway, University of London (2009).