WiP: Applicability of ISO Standard Side-Channel Leakage Tests to NIST Post-Quantum Cryptography

Markku-Juhani O. Saarinen, PQShield LTD, Oxford UK. mjos@pqshield.com

In Brief

- FIPS 140-3 is the primary standard defining security requirements for cryptographic modules in US and Canada. It is generally required for Government use.
- The scope of FIPS 140-3 will also cover the new NIST Post-Quantum Cryptography (PQC) algorithms.
- FIPS 140-3 is introducing testing requirements for Non-Invasive (i.e., Side-Channel) Attack Mitigations.
- ISO 17825 is derived from the statistical methodology used in Test Vector Leakage Assessment (TVLA).
- We discuss ways to apply ISO 17825 to the likely lattice-based PQC standards – Key Encapsulation Mechanisms (KEMs) and Digital Signatures.
- Provides testing coverage for Differential Power (DPA), Differential Electromagnetic Emissions (DEMA), and Timing Attack (TA) mitigations.
- Leakage detection tests can produce false positives. For security "necessary but not really sufficient."

FIPS 140-3 and Side-Channel Testing

The U.S. & Canadian standard for the security of cryptographic modules is FIPS 140-3 (2019); after two decades, validation of implementations to the older FIPS 140-2 standard ended in 2021. The newer standard states that:

> *Major changes in FIPS 140-3 are limited to the introduction of non-invasive physical requirements.*[a]

Non-invasive physical attacks use external physical measurements to derive secret information. They can't modify the module's state. They are commonly known as Side-Channel Attacks (SCA). Many have been developed since the 1990s:

- Timing Attacks (TA) [Ko96].
- Power Side Channels (SPA,DPA) [KoJaJu99].
- Electromagnetic Emission (SEPA,DEMA) [QuSa01].

Post-Quantum Transition of FIPS 140-3

FIPS customers are currently starting to transition from RSA and ECC algorithms to Post-Quantum Cryptography:

- PQC Digital Signature Algorithms.
- PQC Key Encapsulation Mechanisms (KEMs).

The architecture of new high-assurance cryptographic modules (especially for Government use) needs to simultaneously meet both SCA and PQC requirements from now on.

We needed to anticipate the SCA testing procedures in order to create PQC hardware that meets these requirements.

[a] However, there have been other substantial changes in FIPS 140 testing, such as the significantly more comprehensive entropy source requirements [SP 800-90B].

Standard metrics, tools, techniques

Reproducibility: The standards must define test tools, techniques, calibration methods, and apparatus. These standards are just coming to completion (for "pre-quantum").

We assume that the side-channel acquisition set-up and statistical PASS/FAIL metrics remain consistent for PQC.

ISO/IEC 17825 defines Test Vector Leakage Assessment (TVLA) type *leakage tests*. This is a black box test. Secret key extraction does not need to be demonstrated for a FAIL.

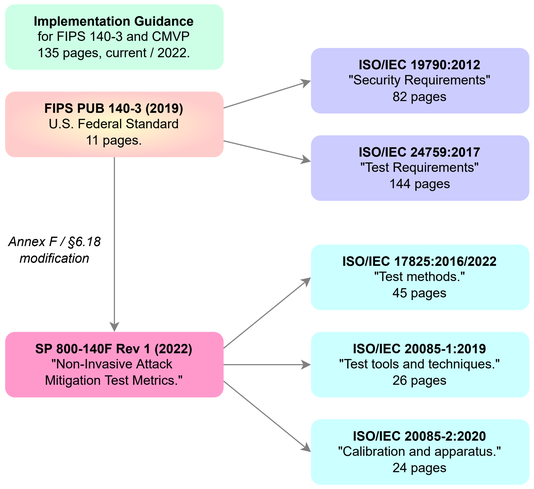

Figure 1: FIPS 140-3 refers a large number of ISO standards, many indirectly. Some of the "working draft" information is hard to find.

On Countermeasures

Masking is considered the most universally applicable countermeasure against side-channel leakage (DPA, DEMA).

- Secret variables (CSPs) are split into randomized shares; observing a subset of shares does not reveal the secret.
- PQC algorithms require a large, varied set of masking "gadgets": Non-uniform samplers, A2B / B2A masking conversions, SHA3/SHAKE, Fujisaki-Okamoto, etc.
- Countermeasures must cover all algorithm components with CSPs, including key management (import/export).
- The area or latency cost of masking can exceed 2×. It can be combined with cheaper (ad hoc) countermeasures.

The General Statistical Test Procedure

ISO/IEC WD 17825:2021(E) includes a "General Statistical Test Procedure" that can be adapted for PQC testing.

Outline of the Procedure:

0. Determine the required sample size $N = N_A + N_B$ and t-test threshold C from the experiment parameters.
1. Collect Subsets A and B and compute their pointwise averages (μ_A, μ_B) and standard deviations (σ_A, σ_B).
2. Compute the pointwise Welch t-test statistic vector
$$T = \frac{\mu_A - \mu_B}{\sqrt{\frac{\sigma_A^2}{N_A} + \frac{\sigma_B^2}{N_B}}}.$$
3. If at any point $|T| > C$, the test results in a FAIL. If the threshold was not crossed, the test is a PASS.

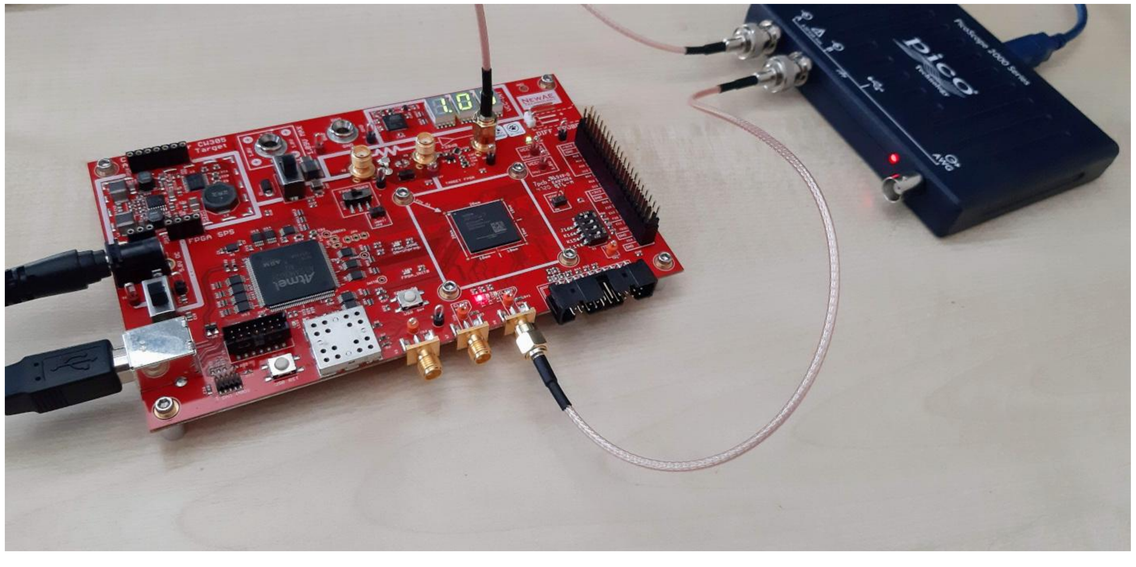

Figure 2: ISO/IEC 20085-2:2020(E) ("Test calibration methods and apparatus") describes the ChipWhisperer 305 FPGA target board in its Annex C. It is used for FPGA leakage emulation of cryptographic RTL. We tested side-channel protected PQC implementations (Kyber, Dilithium, Saber) with it.

Design of Test Vector Sets

We find that simple "random key" vs. "fixed key" tests (as used for AES) can be problematic due to the close linkage between public and private components within PQC keypairs.

Each test vector has algorithm-dependant CSP differences in subset A and subset B inputs. Examples of specific tests:

- **CPA.SD**. KEM Decryption Secret Key Distinguisher.
- **CCA.PC**. KEM Decapsulation (Fujisaki-Okamoto) Plaintext Checking (PC Oracle) distinguisher.
- **SIGN.SD**. Signing secret key distinguisher.
- Keypair Generation, Key Import, or Key Export.

False positives. Detection of non-CSP leakage is a false positive. A non-trivial challenge in creating ISO 17825 testing procedures for PQC is the careful design of test vector inputs so that only relevant CSP leakage is captured in power, electromagnetic, and timing measurements.

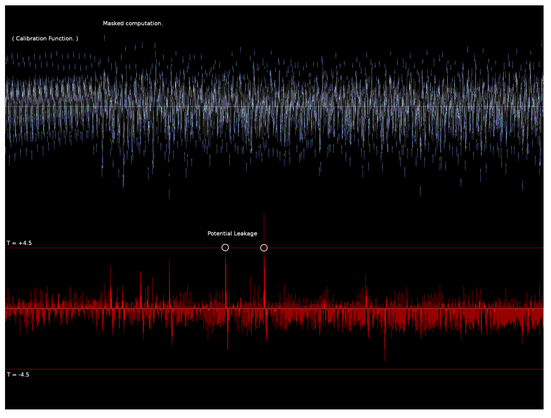

Figure 3: Trace averages and the t-statistic (red) visualized with the time axis. Knowledge of "Spike Cycle" locations ($|T| > C$) help debugging.

Short Paper Reference

Markku-Juhani O. Saarinen: *"WiP: Applicability of ISO Standard Side-Channel Leakage Tests to NIST Post-Quantum Cryptography"*. HOST 2022 WiP Track (2022).

Preprint: `https://eprint.iacr.org/2022/229`

PQSHIELD