

PQC Side-Channel Leakage Assessments in the Semiconductor Industry



9th ETSI/IQC Quantum Safe Cryptography Event
February 15, 2023 - Sophia Antipolis, France


Dr. Markku-Juhani O. Saarinen

Staff Cryptography Architect, PQShield Ltd
Professor of Practice, University of Tampere

Outline

PQC Hardware IP: How to measure side-channel security?

1. Recap: NIST/FIPS/CNSA Post-Quantum Cryptography Standards.
2. Side Channel Attacks: FIPS 140-3 (ISO 17825) vs. Common Criteria.
3. SCA Signoff: Identify secret variables (CSPs), measure leakage.
4. External Laboratory Evaluation & Conclusions.

Note: I only have 15 minutes so this is a helicopter view only 

Recap: (July 2022) NIST PQC = FIPS 140-3 PQC

Post-Quantum Crypto transition is driven by NIST/FIPS

NIST Post-Quantum Crypto: Selected July 2022, Standards 2024.

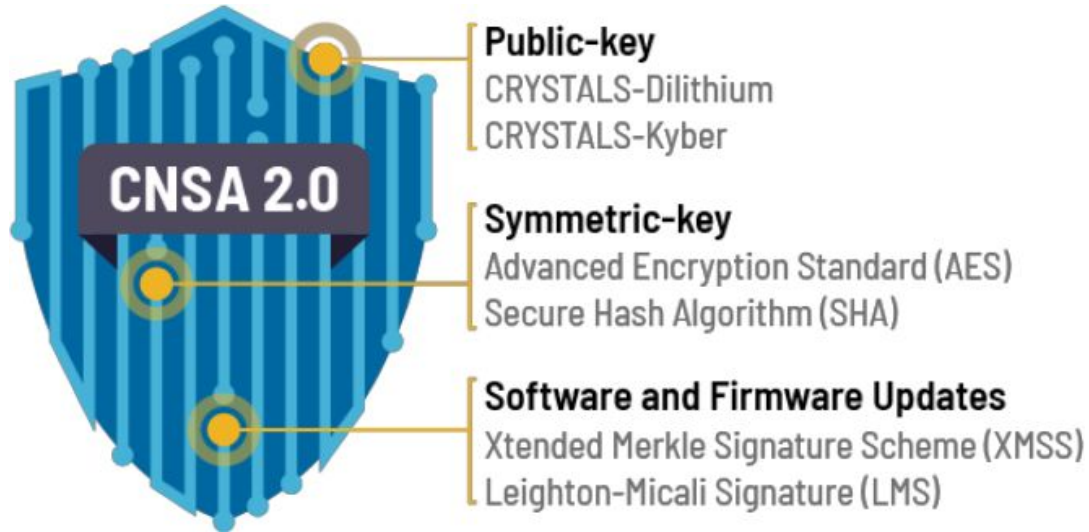
Kyber (+ possibly others) replaces for ECC, RSA key establishment.

Dilithium, Falcon, SPHINCS+ replaces ECDSA, RSA signatures.

Especially for U.S. Government Entities:

- *Active transition effort expected (presidential directives NSM-08, NSM-10).*
- *Regulations mandate FIPS 140-3 cryptography -> also for PQC modules.*

Recap: (September 2022) CNSA 2.0 / NIAP



Transition 2025-2030-2035:

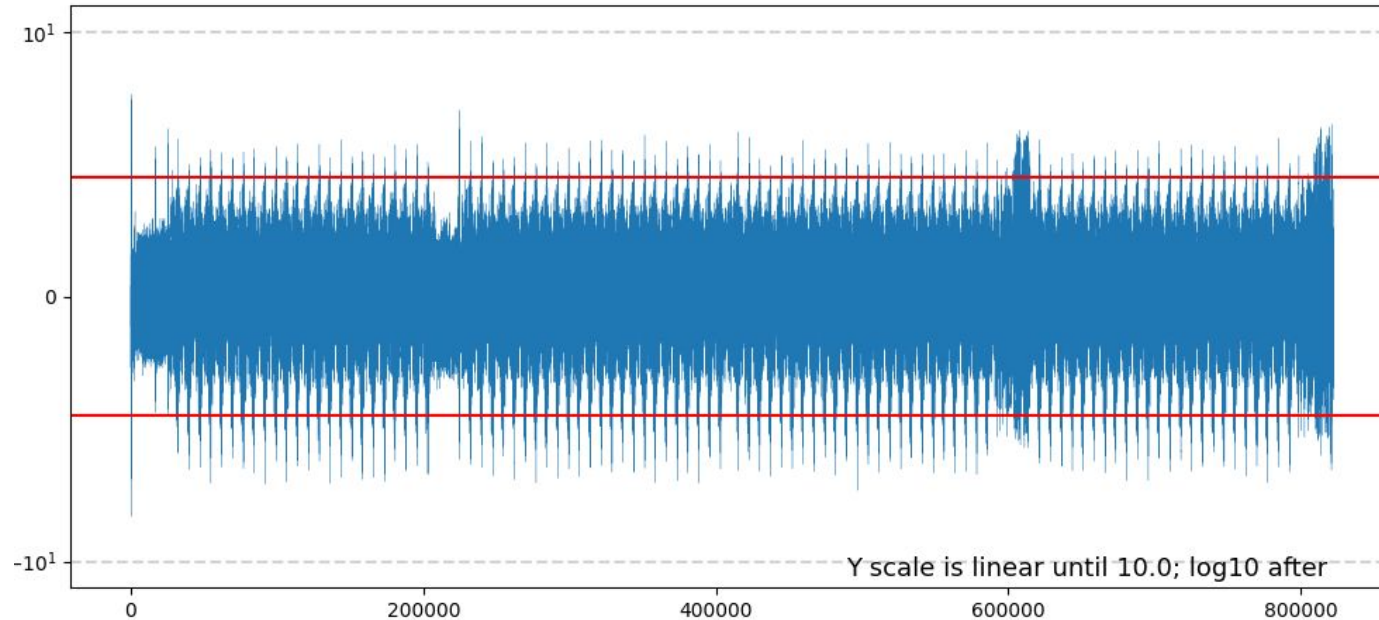
“Note that this will effectively deprecate [in NSS] the use of RSA, Diffie-Hellman (DH), and elliptic curve cryptography (ECDH and ECDSA) when mandated.”

Table III: CNSA 2.0 quantum-resistant public-key algorithms

Algorithm	Function	Specification	Parameters
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.

Physical Side-Channel Attacks

PQC in Smart Cards, Secure Elements, Platform Security, HSMs, etc



- Many applications require security against SCA: We trust that e.g. cell phones retain security even if an adversary gains physical access (or proximity.)
- New PQC Modules inherit the security requirements of ECC/RSA Modules.
- Main attacks are: **DPA: Power**, **DEMA: Electromagnetic Emissions**, **TA: Timing**.

Side Channels: FIPS 140-3 vs. Common Criteria

Standardized Checks vs. Penetration Testing

- **FIPS 140-3** (“Security Requirements for Cryptographic Modules”) Mostly a checklist / functional testing approach. Levels 3 and 4 mandate “*non-invasive attack mitigation*” testing “*if claimed.*”
- **Common Criteria (CC)** can mean many things! High-assurance **Protection Profiles (PP)** contain **AVA_VAN.4** or **.5** (Advanced) methodical vulnerability analysis with “*attack potential*” scores.
- **NSS (U.S. DoD / IC) NIAP** also defines Common Criteria Protection Profiles, but borrows many things from FIPS testing.

SP 800-140Fr1 & New ISO 19790 → ISO 17825

UNCLASSIFIED / NON CLASSIFIÉ

ISO/IEC WD 19790:2022(E)

Annex F (normative)

Approved non-invasive attack mitigation test metrics

Purpose

This Annex provides a list of the ISO/IEC approved non-invasive attack mitigation test metrics applicable to this document. This list is not exhaustive.

This does not preclude the use of approval authority approved non-invasive attack mitigation test metrics.

An approval authority may supersede this Annex in its entirety with its own list of approved non-invasive attack mitigation test metrics.

F.1.1 Non-invasive attack mitigation test metrics

- a) ISO/IEC 17825 *Information technology – Security techniques – Testing methods for the mitigation of non-invasive attack classes against cryptographic modules.*

New ISO 17825 (Nothing specifically on PQC)

Single user licence only, copying and networking prohibited.

DRAFT INTERNATIONAL STANDARD ISO/IEC DIS 17825

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on:
2023-01-25

Voting terminates on:
2023-04-19

Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

Technologie de l'information — Techniques de sécurité — Methodes de test pour la protection contre les attaques non intrusives des modules cryptographiques

PQC SCA Sign-Off / Continuous Integration

Spring 2022: CI starts running (photo of an early set-up in Oxford)



ISO 17825 Leakage Analysis Scenario

DPA and DEMA: Power and Electromagnetic Emission Traces

- **Standard attack setting:** Tester can set inputs to the module at the IO boundary (API). Can choose inputs and synchronize to the start of the operation.
- **Oscilloscope measures power** (or electromagnetic emissions) at high precision, perhaps a couple samples per clock cycle. Measurement vectors are “traces”.
- **Traces are analyzed** to detect leakage. In leakage analysis the analyst can know or choose keys: Is looking for correlations between keys and and the traces.
- **Statistical analysis of significance.** PASS/FAIL metric (no key recovery).

Scope: Critical Security Parameters

Only CSPs are in Scope of “Non-Invasive” (and need masking etc)

Section 7.8 of ISO/IEC 19790:2012(E), unmodified in ISO/IEC WD 19790:2022(E):

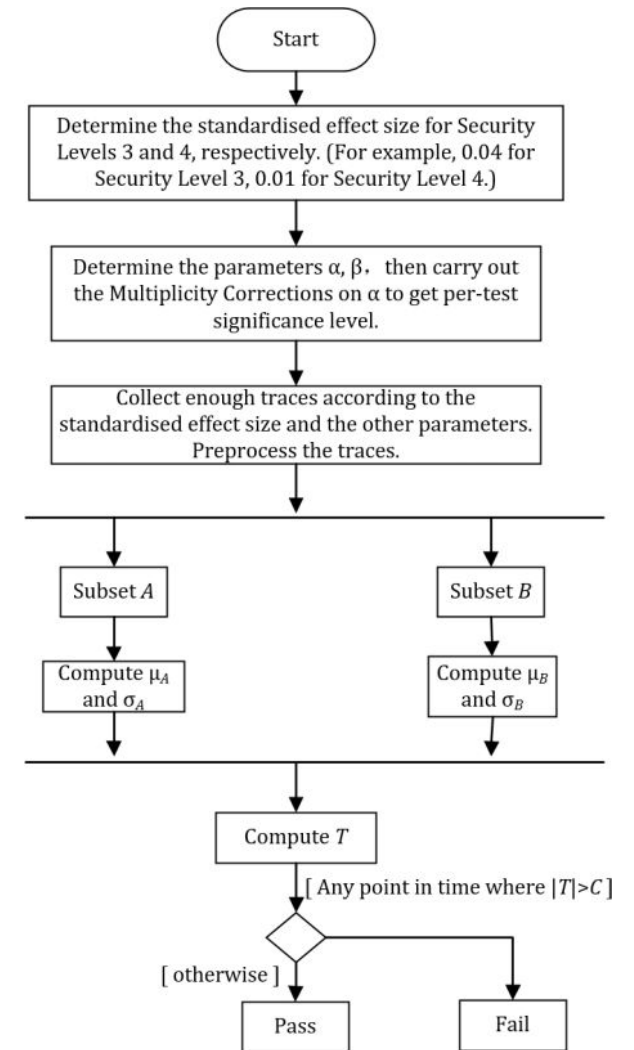
*“Non-invasive attacks attempt to compromise a cryptographic module by acquiring knowledge of the module’s **CSPs** without physically modifying or invading the module. Modules may implement various techniques to mitigate against these types of attacks.”*

- Only leakage of **CSPs** is relevant for FIPS 140-3. Public key leakage is a *false positive*.
- For us, this **CSP** is primarily information that (1) can be used to determine a shared secret in a key establishment scheme or (2) forge a signature in a signature scheme.
- Invasive physical attacks (that modify the state) are out of scope for ISO 17825. FIPS 140-3 has “fault induction mitigation” at Level 4. Faults are a part of CC assessments.

Basic SCA Tests for Post-Quantum Crypto

Detects “leakage” – no key recovery (easily False Positives)

- ISO 17825 has a “general statistical test procedure.”
- The current version of these tests create data subsets A and B of measurements (e.g., trace waveforms) with the IUT.
- But the trace sets A and B need input test vectors!
- **Example:** Set A may use a fixed bit value in a CSP, while measurements in set B use random CSP values.
- If the A/B measurement sets can be distinguished from each other – with the Welch t-test with high enough statistical confidence – this is taken as evidence of CSP leakage.



Two basic types of test vectors will get you far

Fixed vs Random (“FIX”) and A/B Classification (“ABC”)

- 1. Fixed vs Random** (non-specific t-test) can be used in “live” testing:
 - Trace set A: Fixed CSP for every trace.
 - Trace set B: New random CSP secret for each trace.
- 2. A/B Categorization** works with capture-then-analyze flow:
 - Records traces with detailed test vector metadata; CSPs are known in analysis.
 - Traces are categorized *after capture* to A and B sets based on CSP selection criteria, Examples: a specific internal CSP variable or secret key bit, “plaintext checking” bit.
 - The same trace data can be categorized to A and B in a number of different ways.

In both cases: Set A and Set B statistically differentiable with t-test = **FAIL**.

Goals of Automatic TVLA “Sign-Off”

Leakage tests should aim for widest possible coverage

1. Try to have specific testing coverage over all CSPs in all relevant sub-algorithms.

(Key Generation, Key Export, Import, Encapsulation, Decapsulation, Signature.)

2. Design the experiments and test vectors (input data) in a way that eliminates false positives to greatest extent possible.

(Hopefully no need to specify “areas of interest” in resulting traces.)

Opinion: Industry will need to agree on a standardized set of test vectors in order to have consistent results. These are dependant on details of each algorithm.

Third Party Evaluation

Ever-Continuing Process – Developing Industry Best Practices

We're working with Riscure (a well-known 3rd party security testing laboratory) to evaluate our testing methods and the reports issued to semiconductor customers.

November 2022 to assess the physical lab setup at as the second step of the project. This report summarizes the outcomes of these two activities performed in Delft and Oxford respectively.

Based on our assessment of the internal evaluation report, PQShield follows industry best practices to showcase base level first order side channel resistance of their post-quantum crypto implementations. The report includes sufficient details on the choices made for both the evaluation

"Based on our assessment of the internal evaluation report, PQShield follows industry best practices to showcase base level first order side channel resistance of their post-quantum crypto implementations"

"In conclusion, the test methods PQShield uses for gaining a base level assurance on the side channel attack resistance of the implementations in a continuous integration environment is logical and follows industry best practices"

(But methodology needs to be continuously developed.)

Conclusions: PQC Leakage Assessments

- **ISO 17825 / TVLA leakage tests are useful as a semi-automatic sign-off.**
No key recovery or attack potential score – has different goals from AVA_VAN.
- **Such testing should cover all CSPs** (secret variables), in all functions. But care must be taken to avoid false positives (e.g. detection of PSP variables).
- **Business best practice** (before stable standards): Have a well-known 3rd party lab perform side-channel leakage testing, or at least check your processes.

Caveat: Do not let such testing replace security analysis in the design process!

“When a measure becomes a target, it ceases to be a good measure”.

– Goodhart’s law (of unintended consequences.)

Extra: Non-Invasive & FIPS – it's complicated..

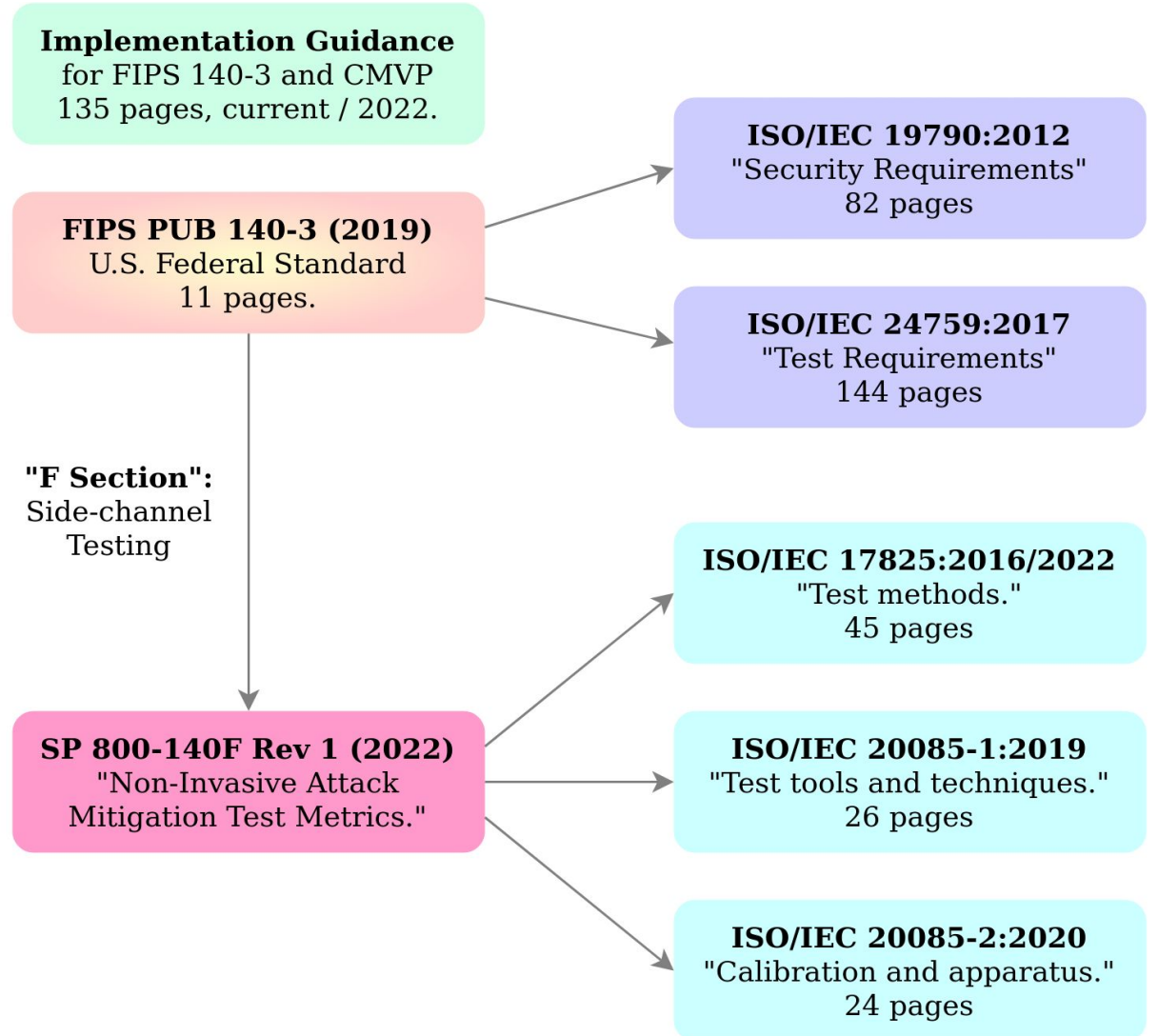
NIST Special Publication		ISO/IEC 19790:2012(E)	ISO/IEC 24759:2017(E)
SP 800-140	modifies	--	§6.1 through §6.12
SP 800-140A		Annex A	§6.13
SP 800-140B		Annex B	§6.14
SP 800-140C		Annex C	§6.15
SP 800-140D		Annex D	§6.16
SP 800-140E		Annex E	§6.17
SP 800-140F		Annex F	§6.18

NIST SP 800-140F Rev. 1 (DRAFT)

CMVP APPROVED NON-INVASIVE
ATTACK MITIGATION TEST METRICS

Document Revisions

Edition	Date	Change
Revision 1	[date]	<p>§ 6.2 Approved non-invasive attack mitigation test metrics</p> <p>Added: ISO/IEC 17825 and associated ISO/IEC 20085-1 and -2</p>



Extra: TVLA / General Statistical Test Procedure

Outline of the General Statistical Test 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 is not crossed, the test is a PASS.