ETSI/IQC Quantum Safe Cryptography Conference 2026

Post-Quantum Agility at Scale: Managing Protocol Evolution and Side-Channel Risk

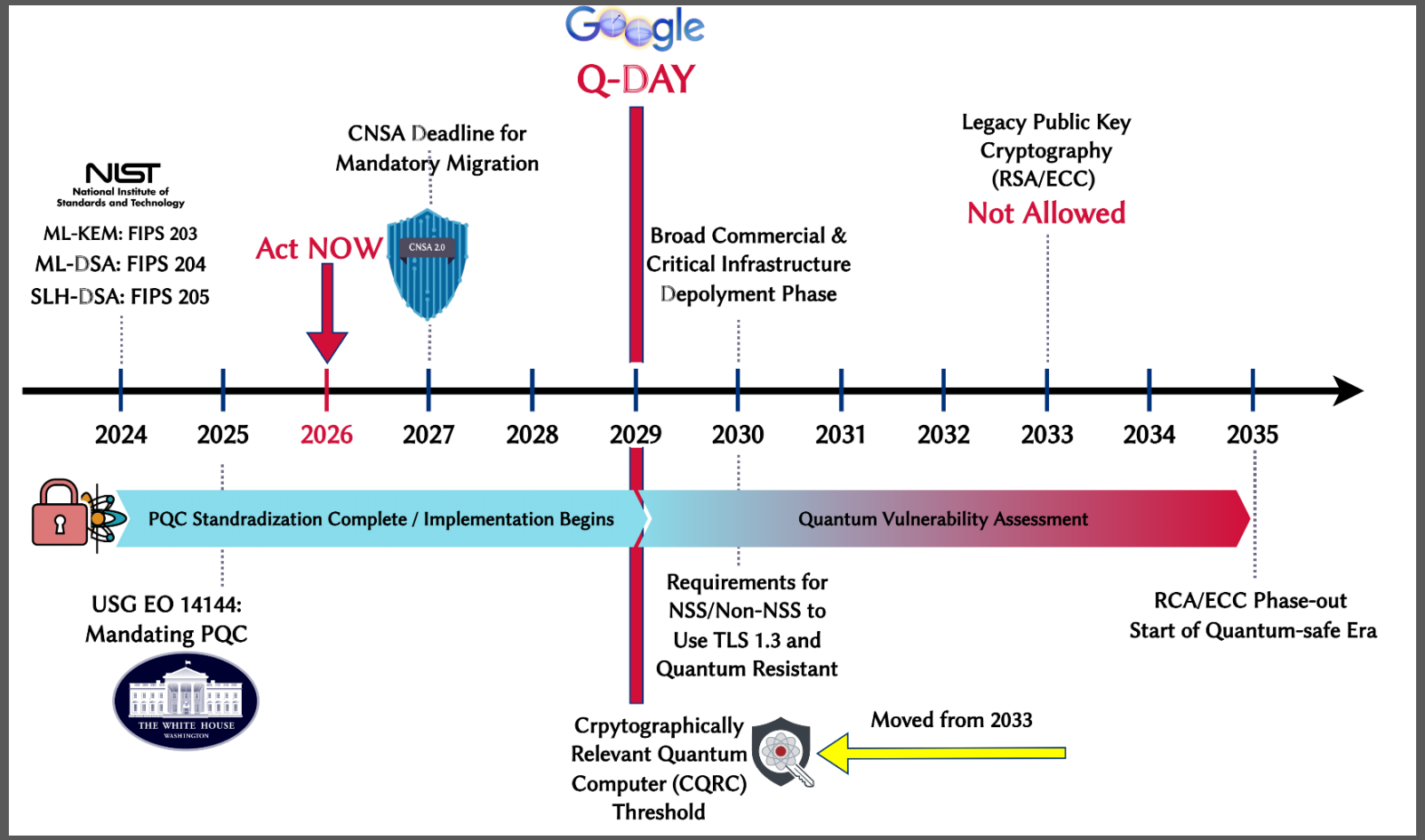
Presented by: Reza Azarderakhsh

06/18/2026

Quantum Mitigation is Achievable
Deployment is the Bottleneck

PQ Secure

"The good news: this problem is solvable today—and PQSecure is already deploying the solution."



PQC for Aviation

PQ Secure

Request for Information:
Post Quantum Cryptography Support for FAA Information Technology and National Air Space Systems (RFI Number 697DCK-26-RFI-PQC)

10 March 2026
Version 1.1

3.1 TECHNOLOGY TIERS SUPPORTED

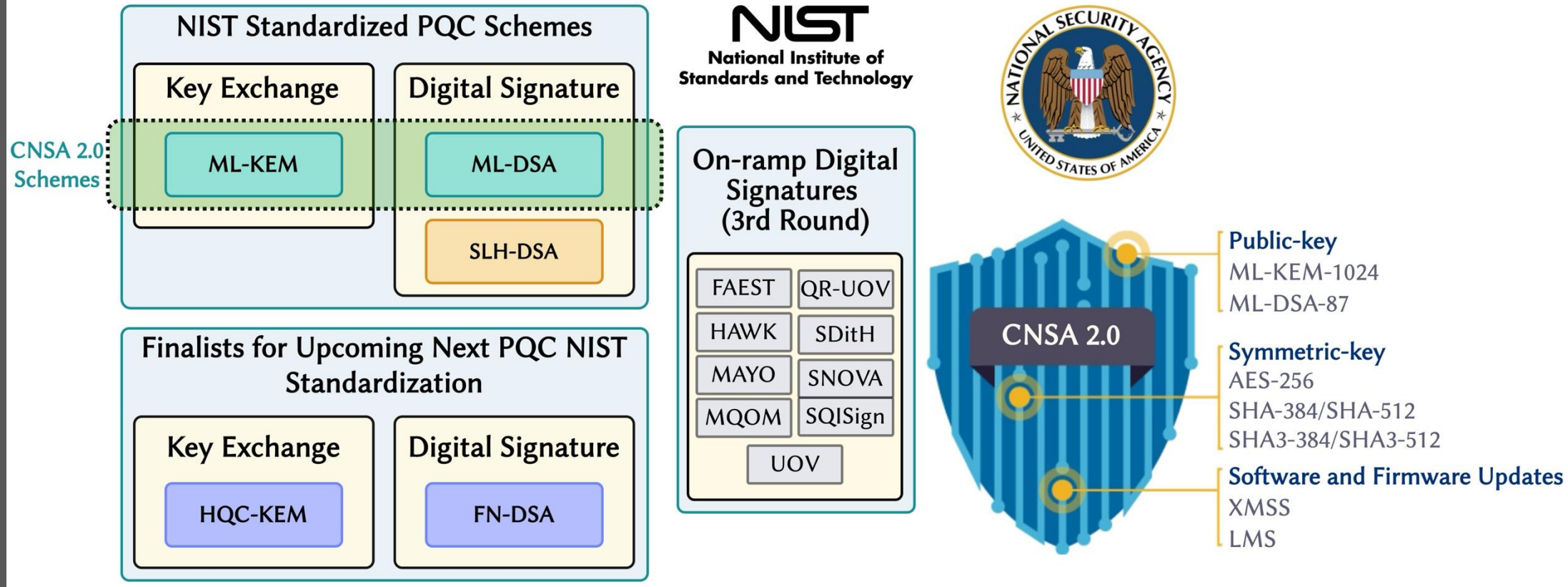
The FAA seeks to understand the impact PQC integration across the following architectural tiers. Respondents should identify which tier or tiers their technology supports and if their solution provides a "One-Stop Shop" (Model A) or a "Component" (Model B). (Table 1)

Table 1: Technology Tiers

Tier	Example Devices/Systems	Envisioned Capability
Root of Trust (Hardware)	HSM Servers, TPM 2.0+, Smart Cards	Hardware-based generation of NIST FIPS 203/204 keys; support for "Hybrid Key Wrapping" (PQC + Classical).
Compute and Infrastructure	Web Servers, App Servers, Database Clusters	CPU-optimized PQC libraries (e.g., OpenSSL 3.5+); support for large-packet handshakes without timeout
Networks and Gateways	VPN Concentrators, Firewalls, SD-WAN	Support for "Hybrid IKEv2/IPsec" tunnels; hardware acceleration (FPGA/ASIC) for line-speed PQC encryption.
Cloud Services	KMS, SaaS Platforms, Virtual HSMs	Managed PQC key lifecycles; interoperability with on-premises PQC roots of trust via standardized APIs.
Edge & Endpoints	IoT Sensors, EFB (Electronic Flight Bags), Avionics	Lightweight PQC implementations for resource-constrained hardware; secure remote firmware signing via SLH-DSA.

PQC Standardization

PQ Secure



FIPS-203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (**ML-KEM**, based on Crystals-Kyber)

FIPS-204: Module-Lattice-Based Key-Encapsulation Mechanism Standard (**ML-DSA**, based on Crystals-Dilithium)

FIPS-205: Stateless Hash-Based Digital Signature Standard (**SLH-DSA**, based on SPHINCS+)

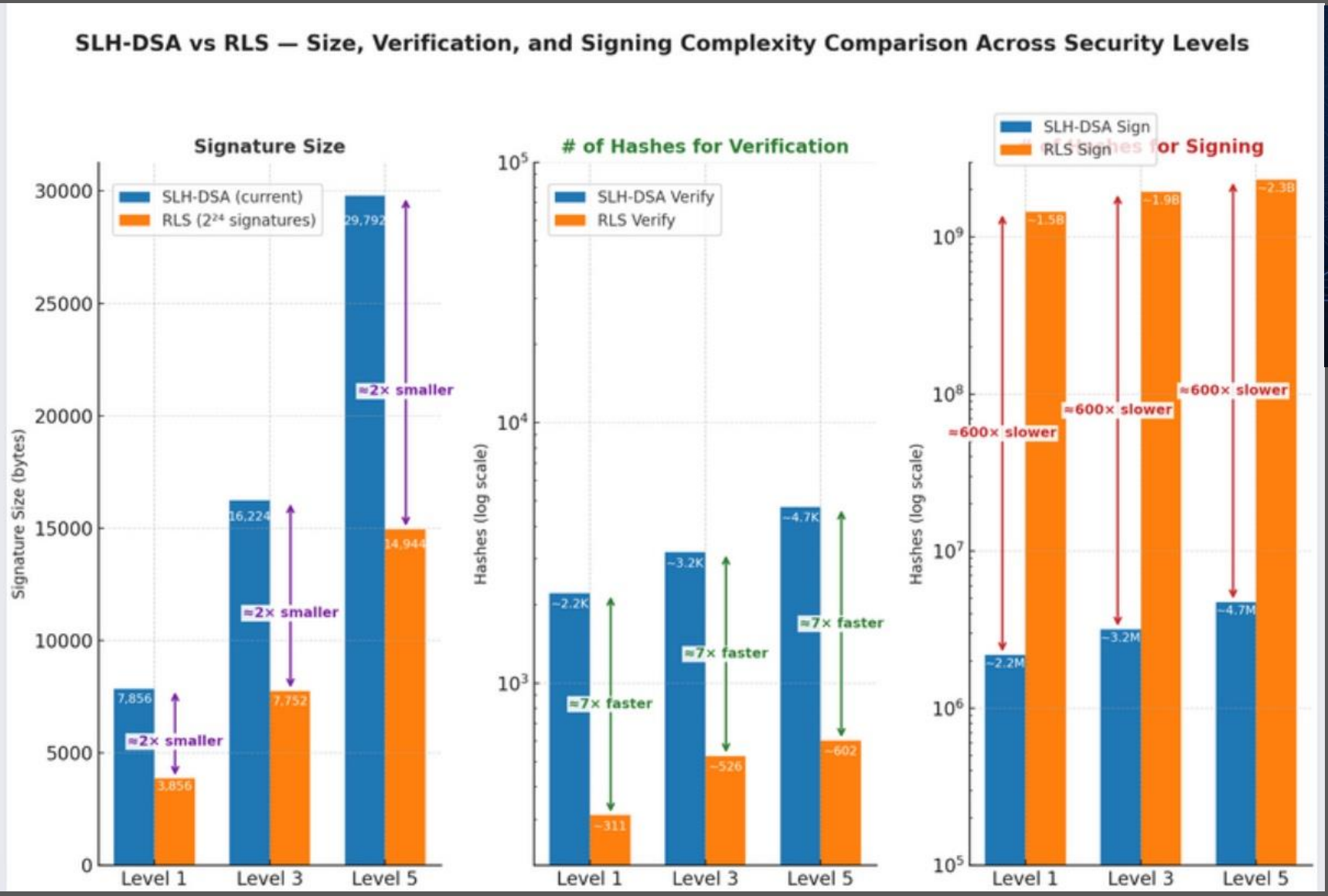
FIPS-206: FFT over NTRU-Lattice-Based Digital Signature Algorithm (**FN-DSA**, based on FALCON)

FIPS-207: Hamming Quasi-Cyclic Key-Encapsulation Mechanism Standard (**HQC-KEM**, based on HQC)

NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes (**XMSS/LMS**)

No-One-Size-Fits-All

PQ Secure



NIST Special Publication 800
NIST SP 800-230 ipd

Additional SLH-DSA Parameter Sets for Limited-Signature Use Cases

Initial Public Draft

Quynh Dang
Dustin Moody

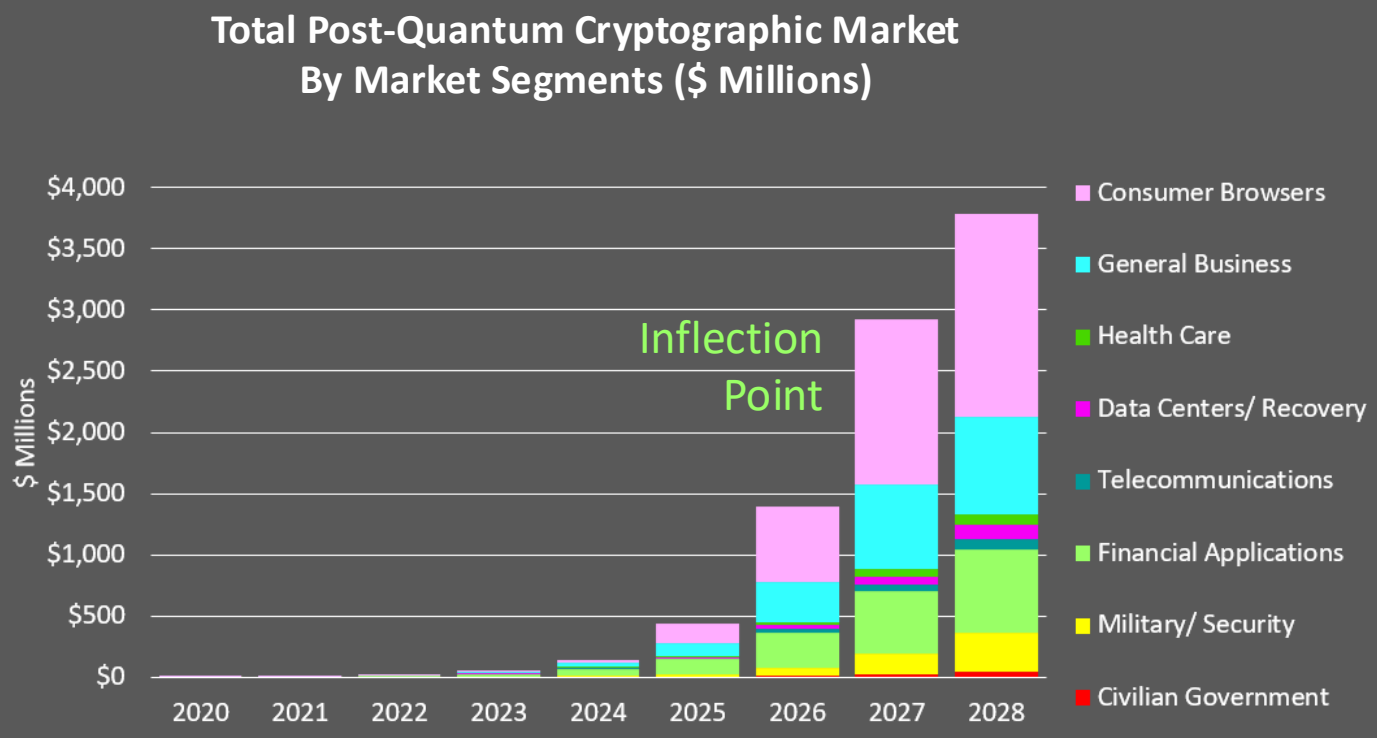
PQ/Cryptographic Engineering

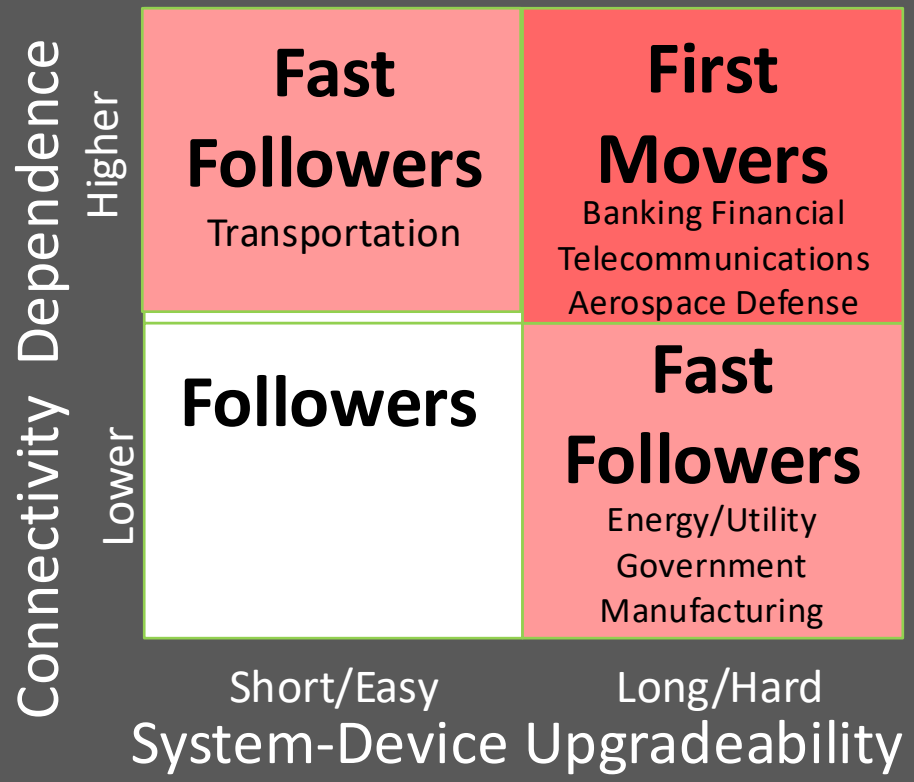
- **I can do it**
  - Experienced in designing SoC with crypto accelerators.
  - Only need IP blocks from PQSecure.
- **Do it for me**
  - Limited resources or expertise, need full support.
  - Require design, integration, and verification assistance.
- **Give me a starting point**
  - Need a secure solution tailored to specific needs.
  - Require customizable IP as a base to avoid reinventing the wheel.

What needs to be upgraded?

All The World's Network-Connected Systems and Devices

PQSecure





PQSecure Is The Foundational Technology For All Devices in All Market Segments*

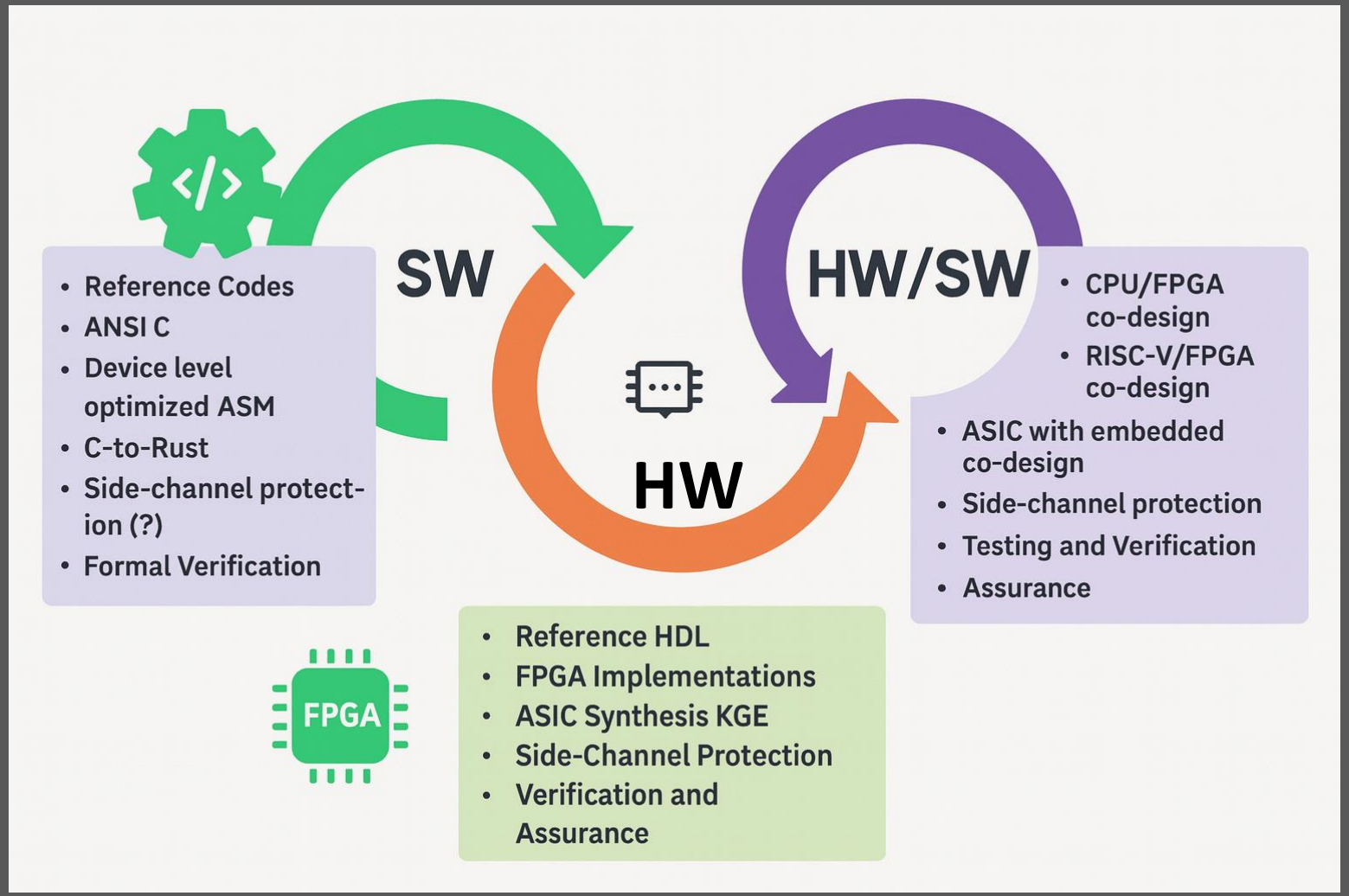
* Source: IQT Insight

High Connectivity, Hard Upgradeability Critical Infrastructure are First Movers**

** Source: 2023 PQSecure Analysis Sponsored by DARPA

SW-First and then HW/SW Co-design

PQ Secure



AUGUST 09, 2022

FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China

Key Strategy 1.1.5: Prioritize hardware integrity and security as an element in co-design strategies across the stack.

In the face of threats from nation-state and criminal adversaries, the potential for the insertion of malicious alterations into components ranging from circuits to software combined with the need to prepare for a post-quantum-computing world make it essential that integrity and cybersecurity be a foundational component of system design.[30,31] Co-design of hardware with software is needed to meet this challenge in a way that provides maximum protection while minimizing the impact on system performance.[32] The design process must allow for iteration between hardware, software, and security constraints. To meet economic and national security needs, security must be incorporated in co-design R&D as a design constraint at the same level as performance.

16

[30] Cybersecurity R&D challenges and goals for hardware and software are described in NITRD's *Federal Cybersecurity Research and Development Strategic Plan* , https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf.

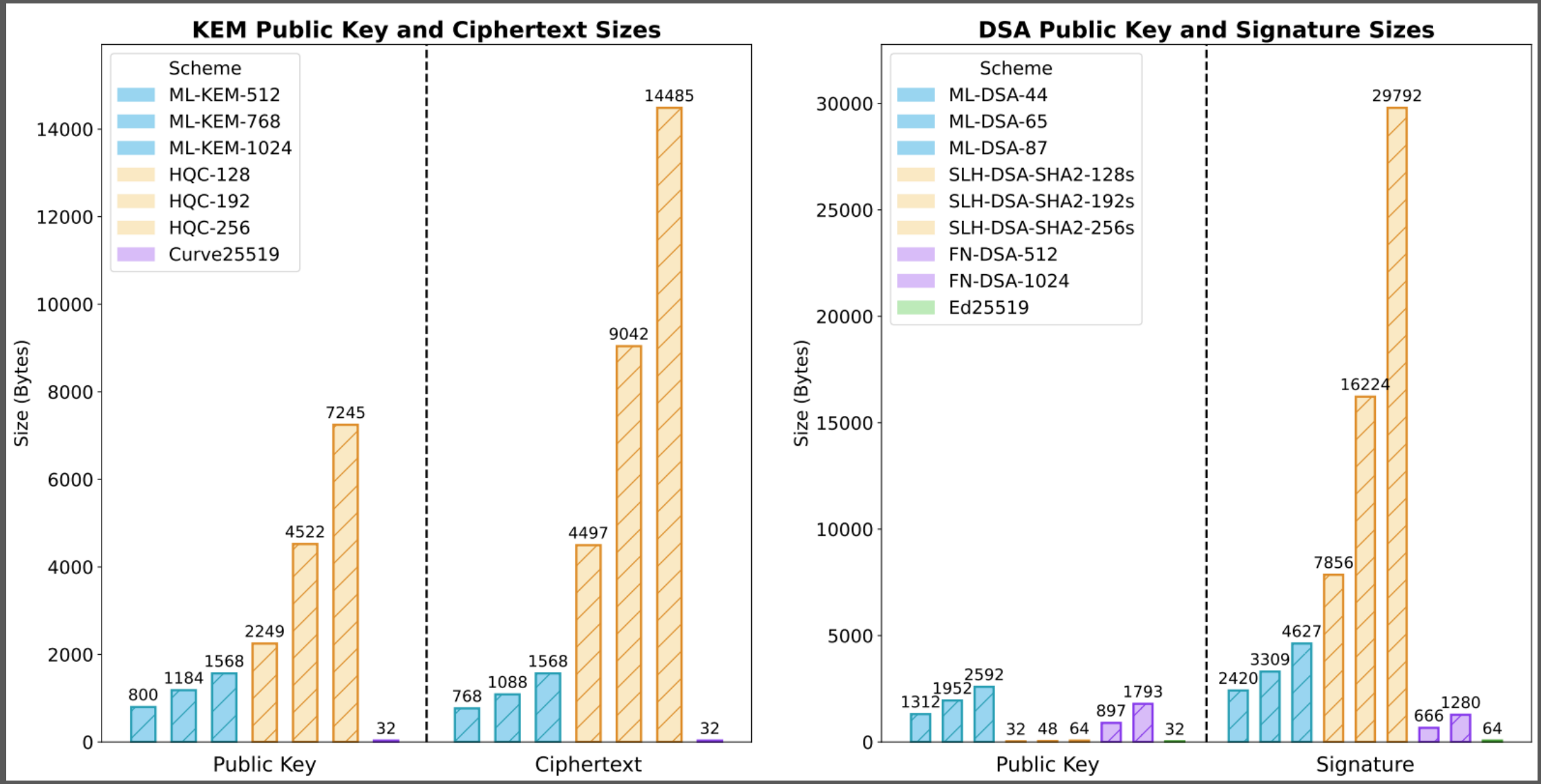
[31] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[32] See, for example, D. Dangwai et al., *SoK: Opportunities for Software-Hardware-Security Codesign for Next Generation Secure Computing*, arxiv.org/abs/2105.00378.

– 12 –

Key sizes for NIST PQC Algorithms

PQ Secure



PQC Agility

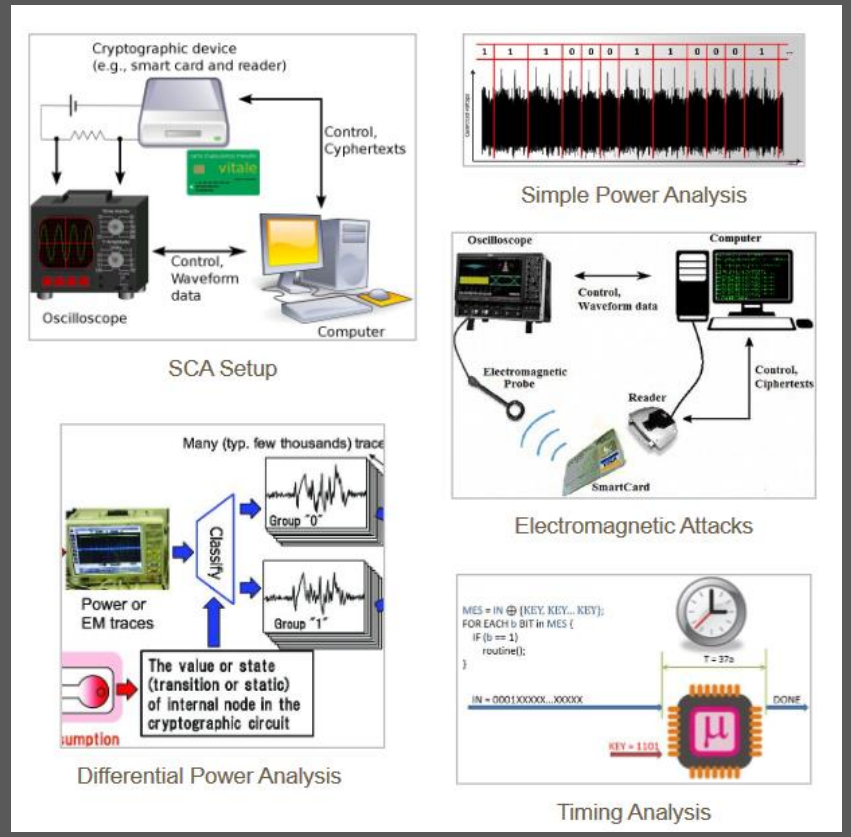
PQ Secure

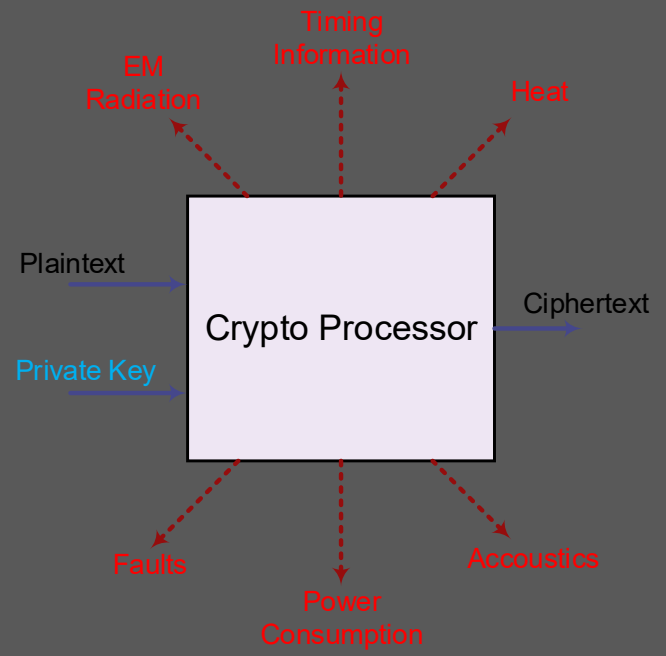
Type of Agility	Definition
Implementation	The Capability to swiftly configure interfaces and implement updates across various systems or applications
Compliance	The capacity to adapt cryptographic configurations in accordance with compliance requirements.
Security Strength	The capability to dynamically adjust the level of security strength based on configuration, allowing for scalable security measures.
Migration	The capability to transition and convert between cryptographic algorithms seamlessly.
Retirement	Ability to retire obsolete or insecure cryptographic algorithms
Composability	The capability to securely integrate multiple cryptographic primitives for composability.
Platform	Ability to use assured cryptographic algorithms across different platform types
Context	Ability to use a derived cryptographic algorithm policy with the flexibility from system attributes

Side-Channel Countermeasures

PQ Secure

- **Simple Power Analysis (SPA)**
- **Differential Power Analysis (DPA)**





(NIST FIPS 140-3 requirement for security level > 3)

What are we talking about?

PQ Secure

Caliptra is an **open-source** hardware Root of Trust (RoT) module bringing many industry specifications together

Caliptra

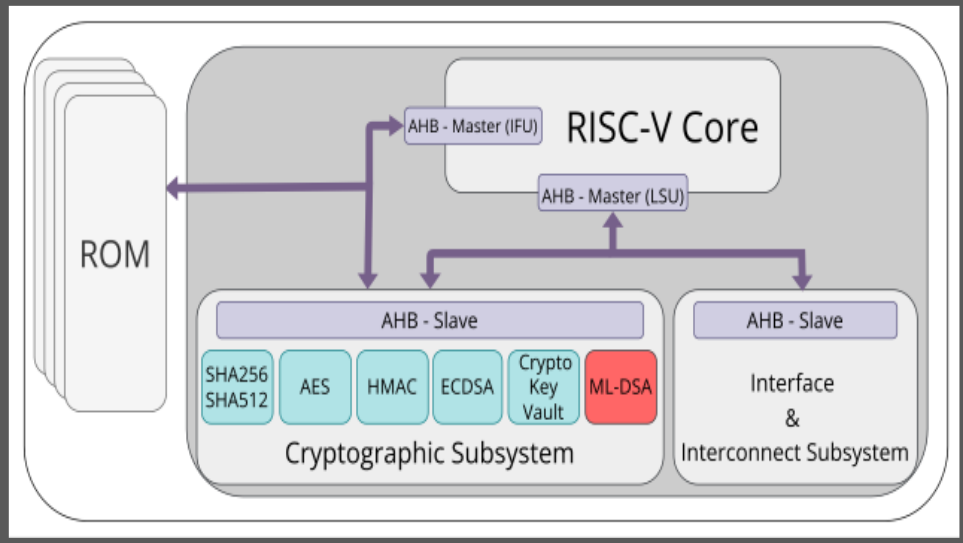
AMD Google Microsoft NVIDIA

- Technical Advisory Council companies committed to deliver products with Caliptra in 2026
- Other ASIC vendors in the pipeline
- Domain experts across EDA, FW, Verification are contributing

Caliptra

PQ Secure

- Caliptra consists of HW/FW IP for a Root of Trust (RoT)
- Caliptra targets datacenter-class SoCs like CPUs and GPUs
- Contains specification, silicon logic, ROM and firmware for implementing a RoT for Measurement (RTM) block inside an SoC
- A Caliptra integration provides the SoC with Identity, Secure and Measured Boot and Attestation capabilities



Caliptra High level block diagram

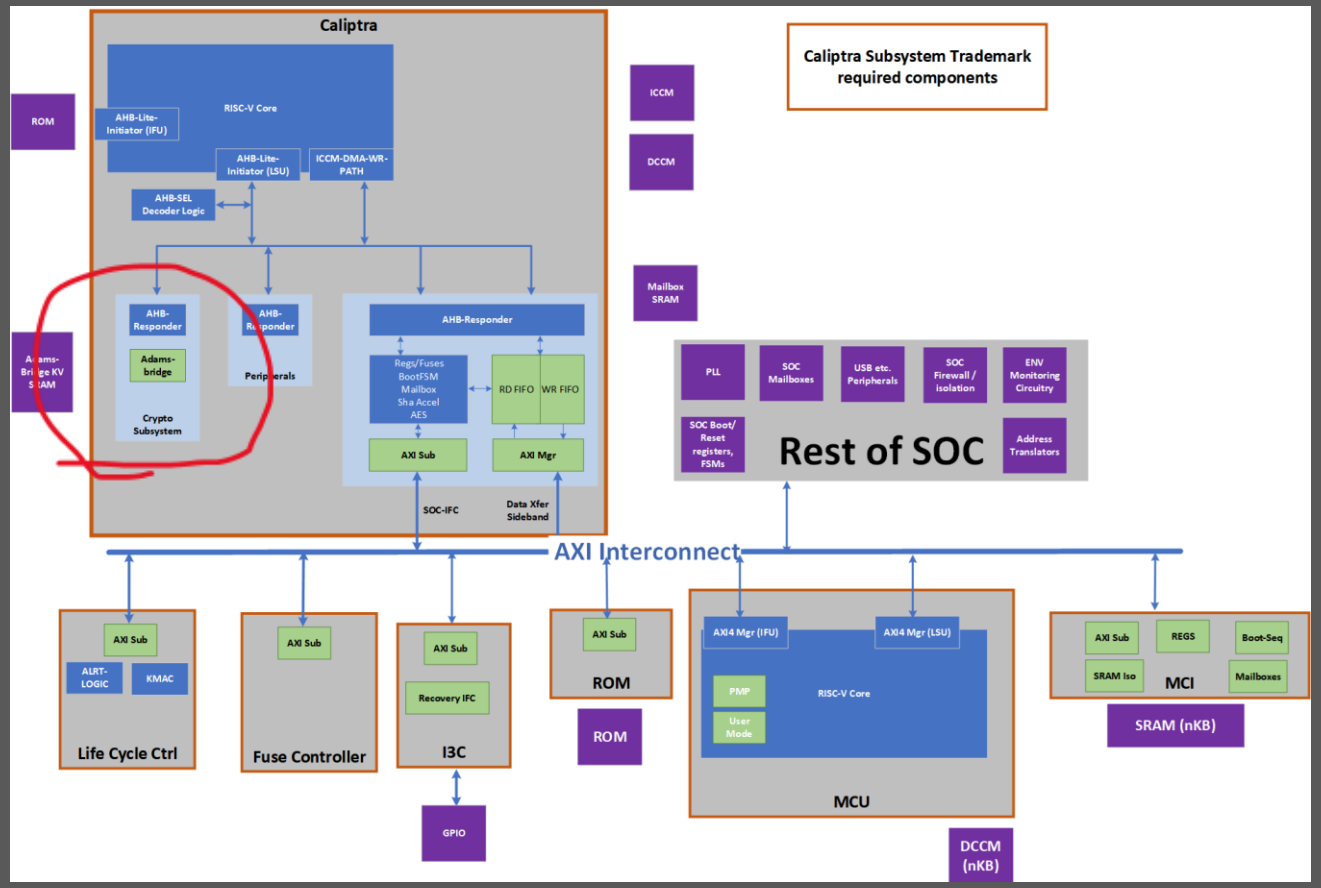
Adams Bridge is an open-source, hardware-accelerated implementation of the ML-DSA (aka Dilithium).

It is responsible for generating and verifying signatures.

Caliptra Subsystems

PQ Secure

- Caliptra 1.X Targeted CMVP Level 1 Certification Ready
  - Minimal Exported Crypto Services
- Caliptra 2.X Targeting CMVP Level 2/3 Certification Ready
  - Significant Increase in Crypto Services



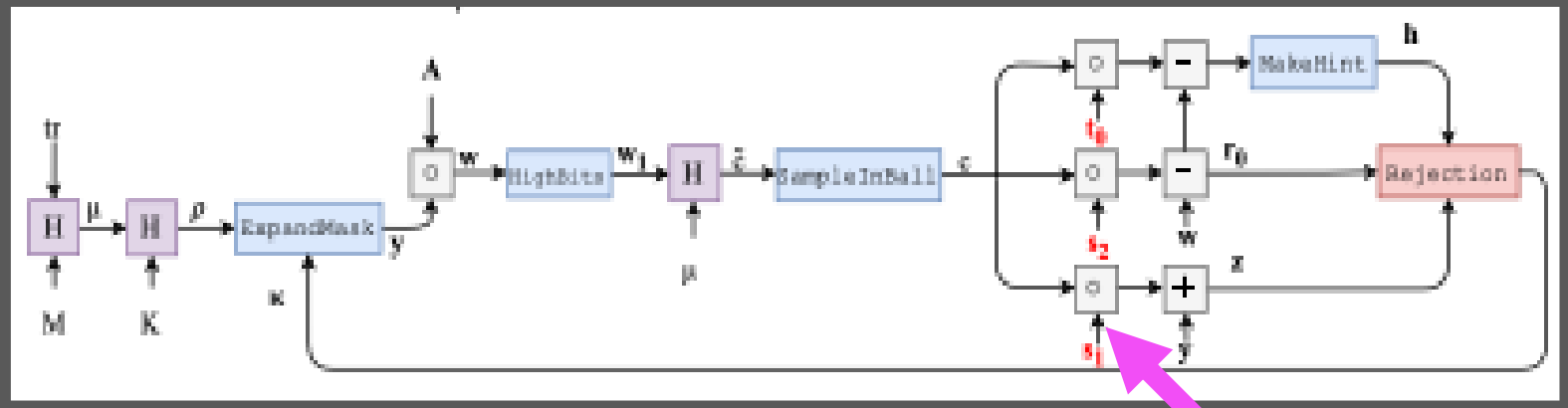
Overview of ML-DSA in Caliptra 1.0

PQ Secure

- **Adam's Bridge: ML-DSA Hardware Accelerator Overview**
  - **47,600+ lines** of publicly available SystemVerilog
    github.com/chipsalliance/adams-bridge
  - Using **v1.0 / v1.0.1 (May 2025)** release
  - Supports only **ML-DSA-87** ("Category 5" Dilithium)
- **Functional Scope:**
  - KeyGen, Sign, and Verify
  - No support for hybrid schemes or algorithmic agility
- **Limitations:**
  - **Non-programmable** — No updates or patching supported
  - Designed as a fixed-function accelerator, not a cryptographic processor
- **Early ML-KEM commits** started in May 2025
  - ML-KEM integration is in infancy and not yet production-ready

Successful CPA attack on Cliptra 1.0

PQ Secure



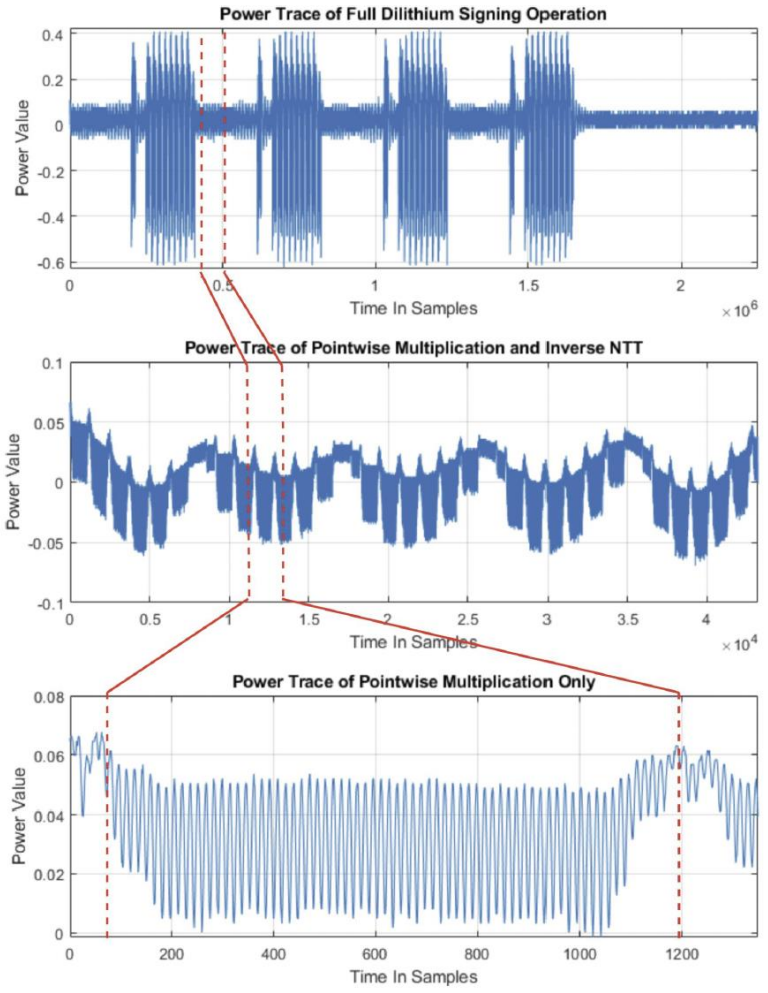
Target operation

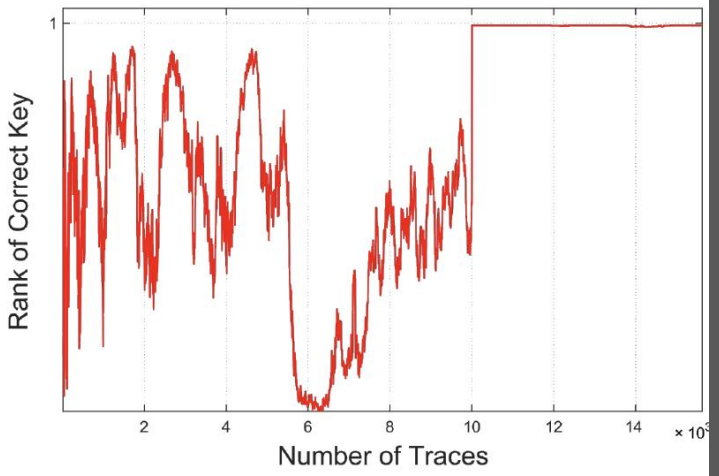
- **Target**: Secret-key multiplication in **ML-DSA-87** Implemented in the **October 2024 release** of Adam's Bridge
- **Platform**:
  - Deployed on **CW305 Artix-7 FPGA testbed**
  - Collected **10,000 power traces** using oscilloscope-based side-channel capture
- **Method**:
  - **Correlation Power Analysis (CPA)** performed on intermediate values
  - Exploited leakage from **unmasked multiplication logic**

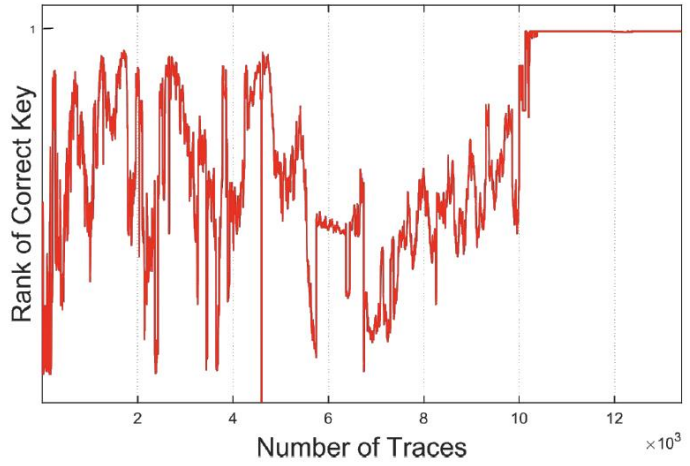
M. Karabulut, R. Azarderakhsh,
"Efficient CPA Attack on Hardware Implementation of ML-DSA in Post-Quantum Root of Trust"
IEEE HOST 2025 — https://ia.cr/2025/009

Attack Setup

PQ Secure







SCA Protected Caliptra 2.0 Overhead

PQ Secure

- **Adam's Bridge: Area Overhead Analysis**
- Protected **ML-DSA-87 core** synthesized at **0.114 mm² @ 5nm**
  - 0.0921 mm² for stdcell logic
  - 0.0220 mm² for **57.38 KB** of RAM
  - Target frequency: **600 MHz**
- Estimated to require:
  - **3 million gate equivalents**
  - **~335K LUTs** for equivalent FPGA implementation
- Compared to typical secure cores:
  - **>30×** larger than ARM Cortex-M3 (100–120K NAND2)
- Other secure ML-DSA implementations:
  - Typically consume **10–30%** of Adam's Bridge size

SCA Protected Caliptra 2.0 Overview

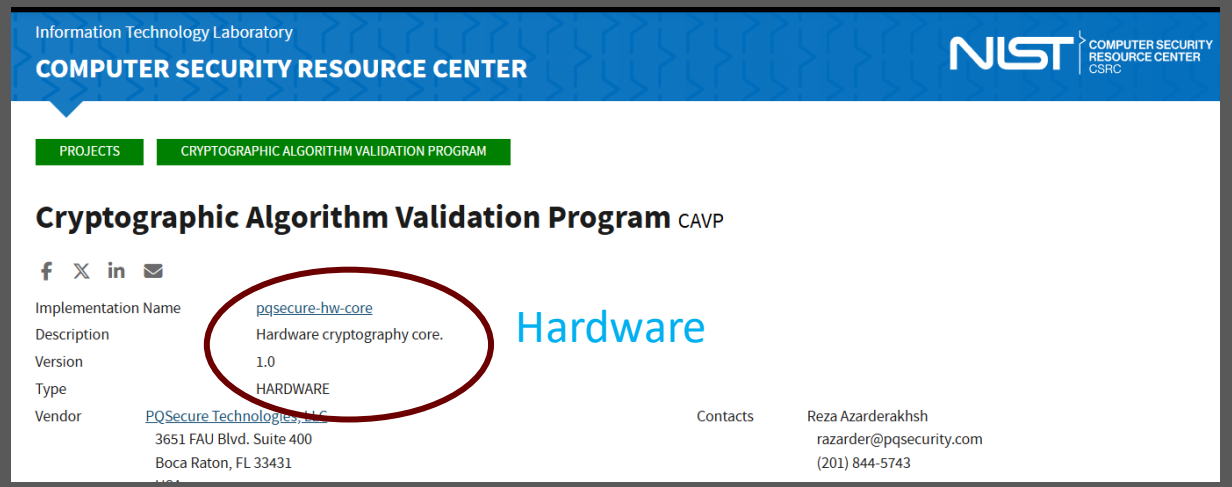
PQ Secure

Sensitive Operation	Protection in Caliptra	Computation Description
NTT(s_1, s_2)	Shuffling only	Converts secret polynomials to NTT domain (FFT-like transform).
A·y	❌ None	Multiplies public matrix A with secret ephemeral vector y.
cs_1, cs_2	Masking only	Multiplies challenge polynomial c with secrets s_1 and s_2.
ct_0	Masking only	Multiplies challenge c with part of the public key t_0.
$NTT^{-1}(cs_1, cs_2)$	Shuffling + Masked 'first state'	Applies inverse NTT to transform results back to time domain.
$y + cs_1$	Shuffling only	Adds ephemeral secret y to challenge-scaled secret s_1.
$w - cs_2$	Shuffling only	Subtracts challenge-scaled s_2 from intermediate result w.
ExpandMask	❌ None	Samples secret y from uniform or centered binomial distribution.
H(K ‖ rnd ‖ mu)	❌ None	Hashing operation used to generate deterministic randomness.
Decomposition	❌ None	Splits coefficients into high and low bits for signature compression.
BoundCheck(z)	❌ None	Verifies that z stays within a predefined rejection bound.
BoundCheck(r_0)	❌ None	Ensures r_0 remains within error bounds after subtraction.
BoundCheck(ct_0)	❌ None	Checks correctness of hint-related computations on t_0.

- Caliptra's current protections are incomplete.
- High-risk components like ExpandMask, BoundCheck, and A·y remain **unprotected**, leaving Caliptra 2.0 **vulnerable to first-order side-channel attacks**.

PQSecure NIST Standards Compliance

- Compliance with NIST FIPS 203/204/205 + CNSA 2.0 + NIAP.



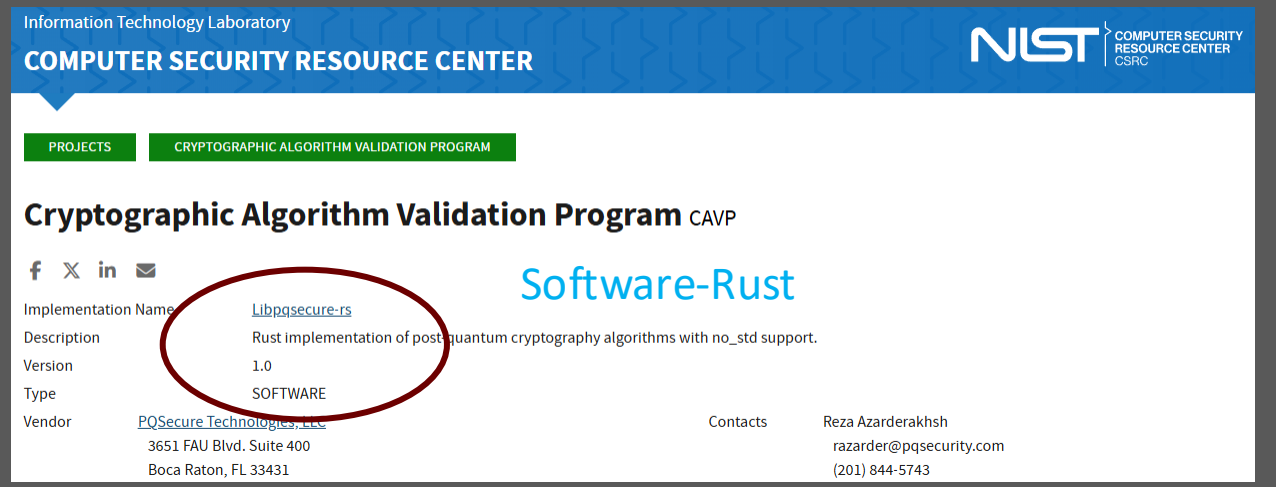
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

Hardware

Implementation Name	pqsecure-hw-core
Description	Hardware cryptography core.
Version	1.0
Type	HARDWARE
Vendor	PQSecure Technologies, LLC 3651 FAU Blvd. Suite 400 Boca Raton, FL 33431
Contacts	Reza Azarderakhsh razarder@pqsecurity.com (201) 844-5743



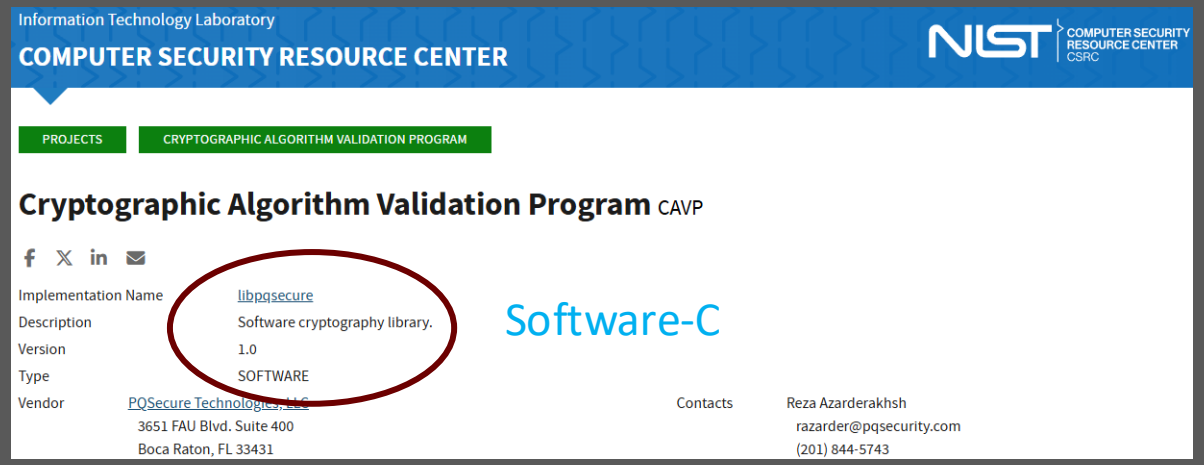
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

Software-Rust

Implementation Name	Libpqsecure-rs
Description	Rust implementation of post-quantum cryptography algorithms with no_std support.
Version	1.0
Type	SOFTWARE
Vendor	PQSecure Technologies, LLC 3651 FAU Blvd. Suite 400 Boca Raton, FL 33431
Contacts	Reza Azarderakhsh razarder@pqsecurity.com (201) 844-5743



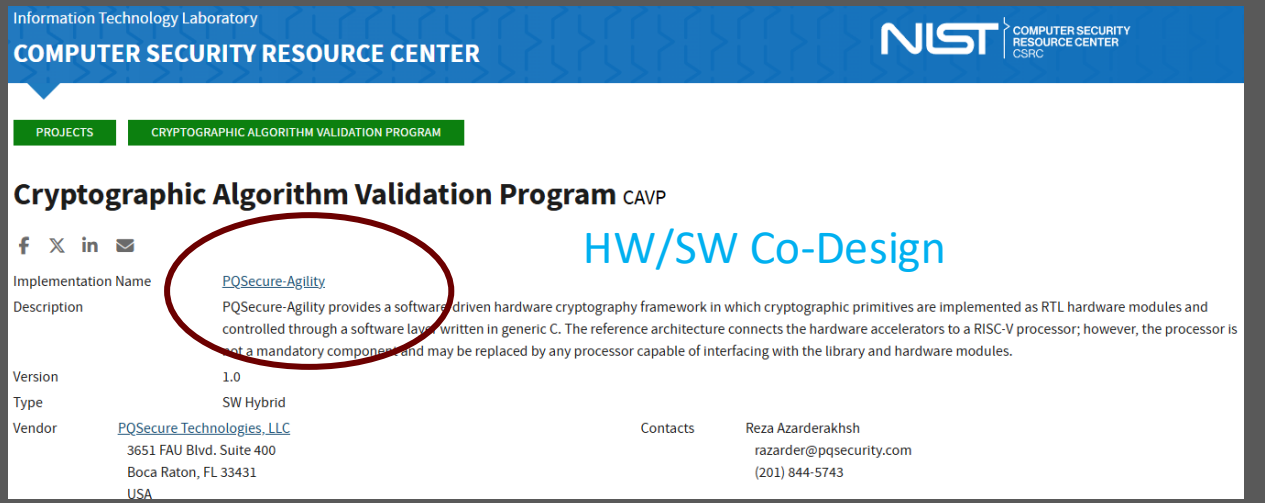
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

Software-C

Implementation Name	libpqsecure
Description	Software cryptography library.
Version	1.0
Type	SOFTWARE
Vendor	PQSecure Technologies, LLC 3651 FAU Blvd. Suite 400 Boca Raton, FL 33431
Contacts	Reza Azarderakhsh razarder@pqsecurity.com (201) 844-5743



Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

HW/SW Co-Design

Implementation Name	PQSecure-Agility
Description	PQSecure-Agility provides a software-driven hardware cryptography framework in which cryptographic primitives are implemented as RTL hardware modules and controlled through a software layer written in generic C. The reference architecture connects the hardware accelerators to a RISC-V processor; however, the processor is not a mandatory component and may be replaced by any processor capable of interfacing with the library and hardware modules.
Version	1.0
Type	SW Hybrid
Vendor	PQSecure Technologies, LLC 3651 FAU Blvd. Suite 400 Boca Raton, FL 33431 USA
Contacts	Reza Azarderakhsh razarder@pqsecurity.com (201) 844-5743

PQSecure Offerings Built on Innovation

PQ Secure

PQ Secure

SW Library IP

C, Rust, performance/memory tiers

SW IP Licenses

HW Silicon IP

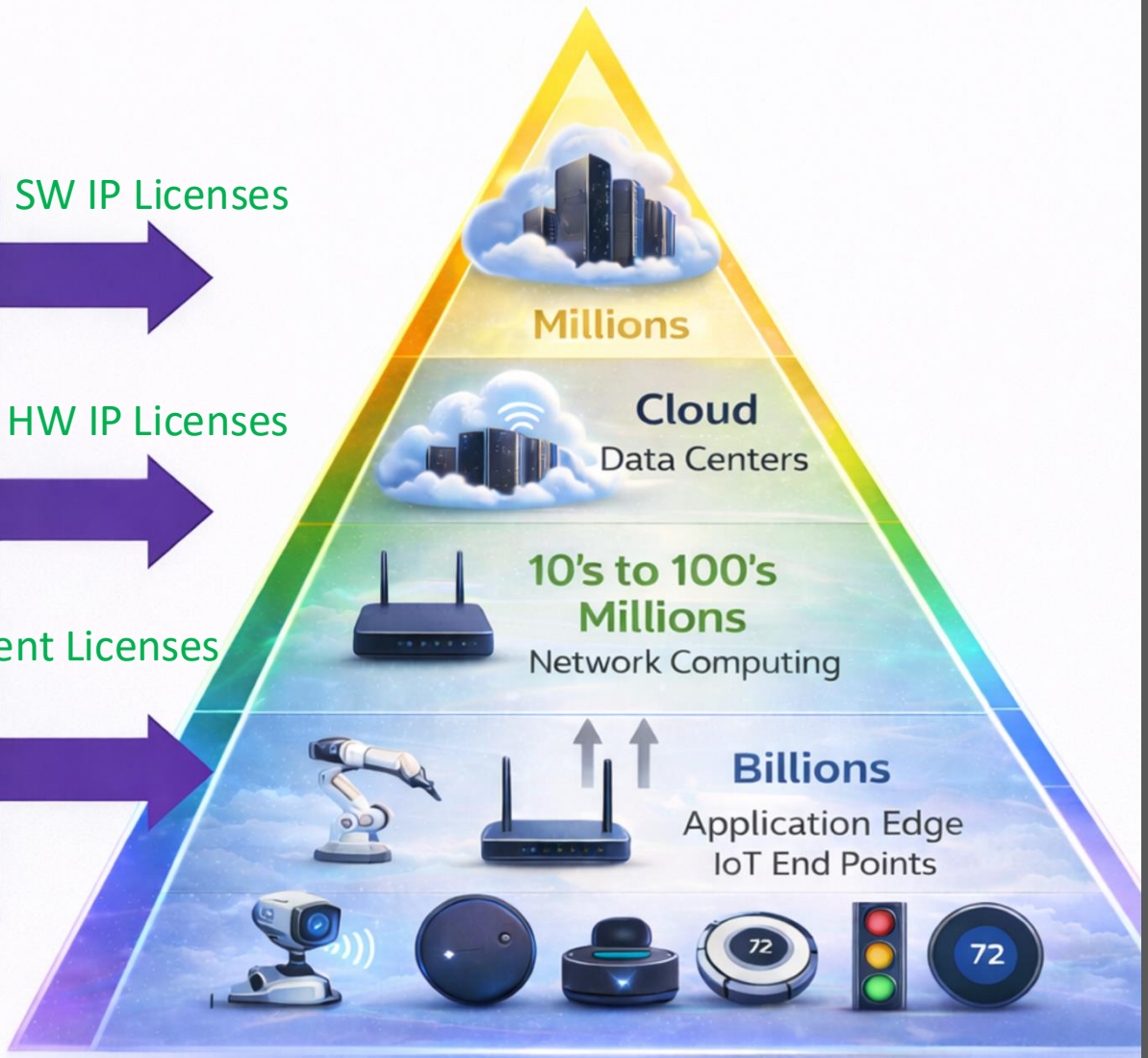
Tiny / Compact / Balanced / Performance

HW IP Licenses

Innovations

Foundational R&D, patents
side-channel R&D
formal verification

Patent Licenses



Questions?

PQ Secure

Reza Azarderakhsh

CEO at PQSecure
Email: razarder@pqsecurity.com