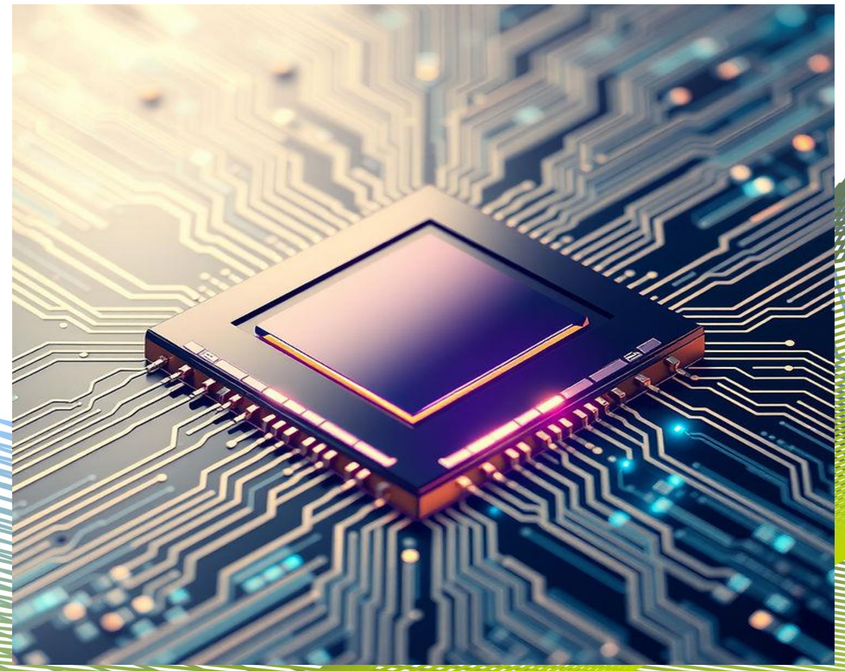
Quantum-Safe Silicon: from Chips to Cyber-Resilient Systems

Prof. (Asst.), Dr. Angelos K. Marnerides
EU FOCAL Project Coordinator
Cyber-Physical Systems Security
Dept. of Electrical & Computer Engineering
KIOS R&I Centre of Excellence
University of Cyprus

TRANSFORM TOMORROW

Post Quantum Cryptography (PQC) is moving into silicon….



TRANSFORM TOMORROW

Why PQC? The threat arrives before the quantum computer…

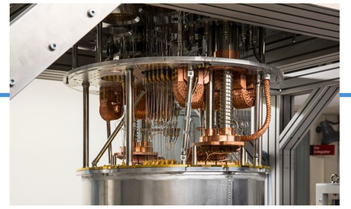
Harvest now, decrypt later….

Today



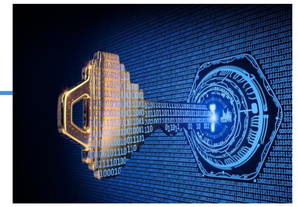
Encrypted data is captured

Few years later



Cryptographically relevant QC

Then



Stored data is decrypted

ciphertext archive → **Q + Shor** → **plaintext**

The quantum computer can arrive in the future, but the security impact can start today.

Why the semiconductor industry should care

- PQC expands the hardware envelope

→ compute, memory, bandwidth and energy.

- Long-lived platforms need crypto-agility

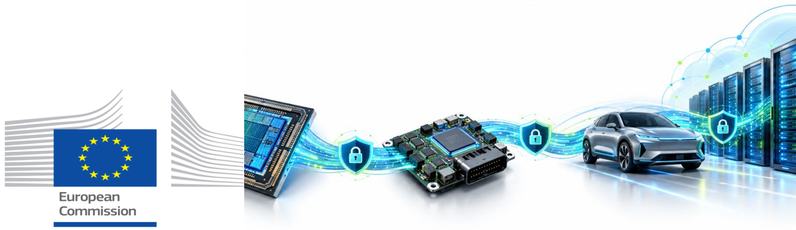
→automotive, industrial and edge devices cannot wait for a future redesign.

- Acceleration + hardware trust decide whether PQC is deployable at scale.



Post-quantum security is becoming a system-architecture problem and not just an algorithm upgrade.

Project: Functional Composition of PQC At Large (FOCAL)
Budget: €6.4M
Duration: 3 years (2025-2028)

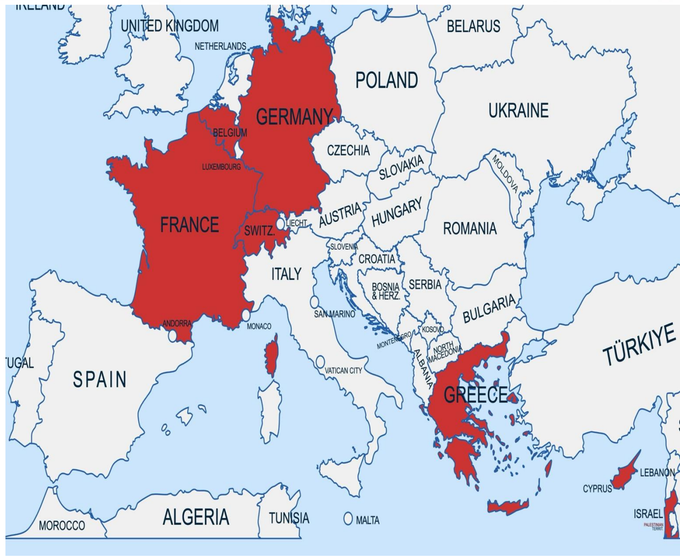


- End-to-End (E2E) PQC Composition
  → chip → edge → cloud

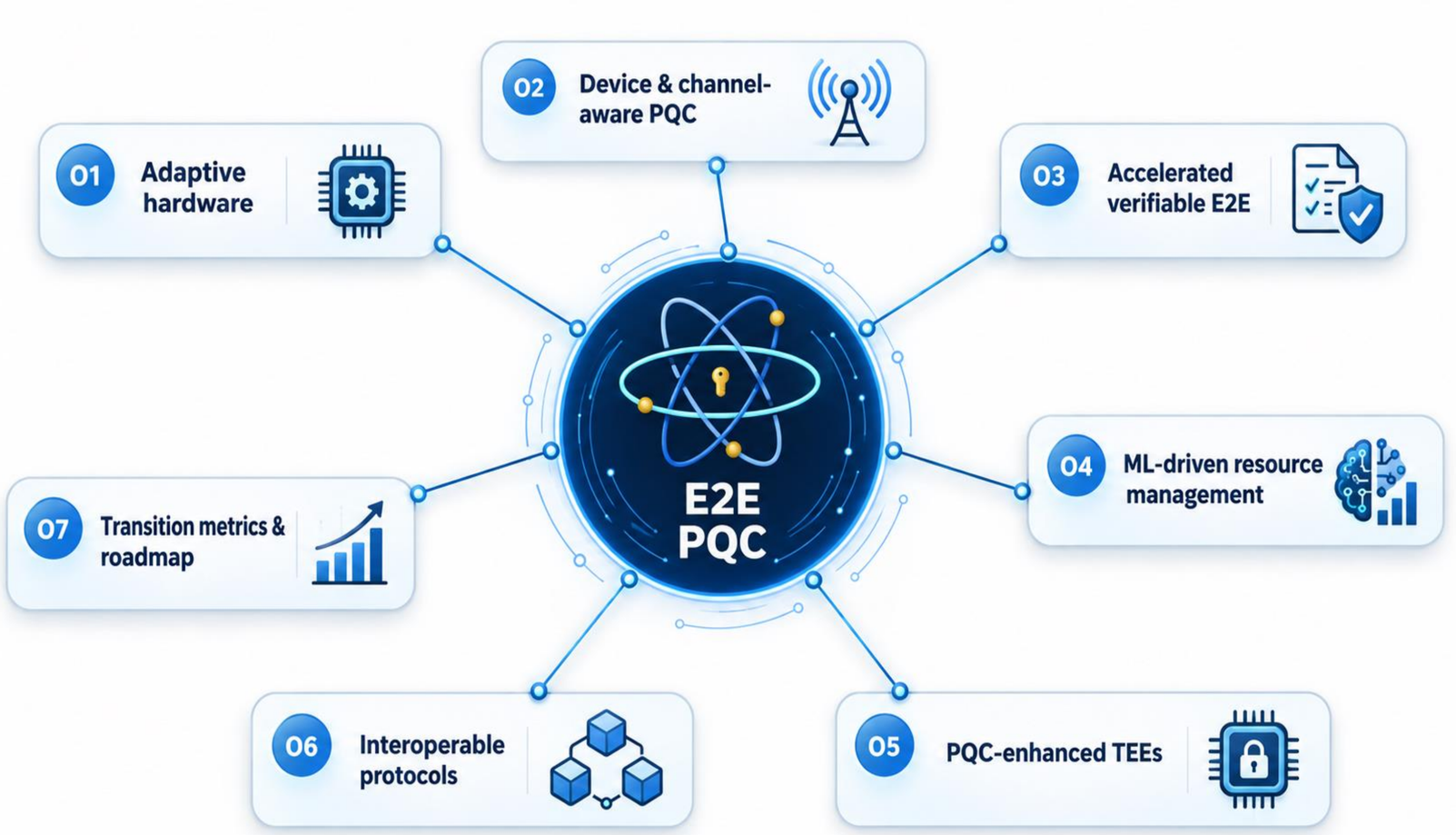
- Mission: make PQC practical across constrained, connected and high-performance systems.

- Co-design — hardware, trusted execution, protocols, networking and orchestration.

- Validate — six real application domains, from automotive and MedTech to data centres.



FOCAL Objectives



FOCAL: a chip-to-cloud PQC stack

1 Silicon + device roots
PQC accelerators, PUF/TRNG roots, area–power–latency trade-offs.

2 Trusted execution + lifecycle
TEEs, attestation, protected keys, secure boot and update.

3 Network + edge
Crypto-agile protocols, eBPF/XDP and SmartNIC/DPU offload.

4 Orchestration + evidence
Deploy, rotate, benchmark and validate across heterogeneous systems.



FOCAL → make quantum-safe security a first-class, updateable hardware and network capability.

Device-level quantum resilience: trust begins inside the chip

FOCAL combines device physics, hardware roots of trust and secure lifecycle mechanisms → PQC is anchored in silicon, not bolted on later.

Spintronic PUF → device identity

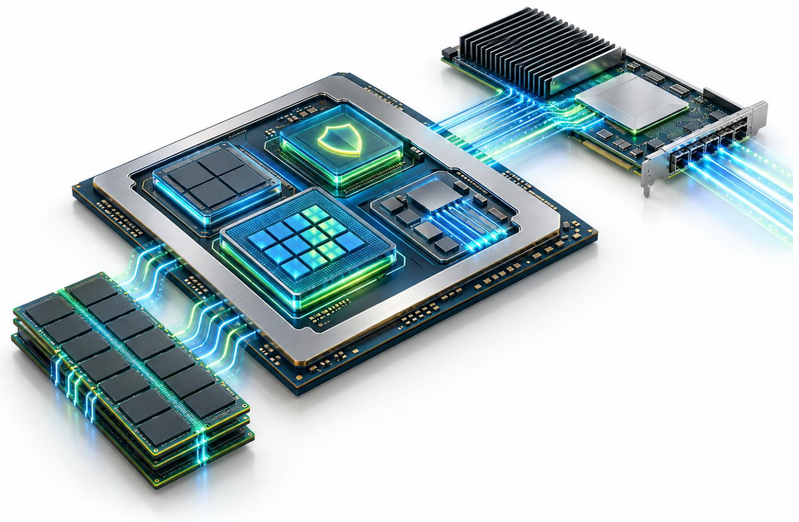
SpinEdge: 16-sMTJ digital twin completed; 8×8 array in progress. Evaluation: entropy, reliability, key-generation rate.

PQC accelerator + TEE → protected keys

NXP i.MX95 / RISC-V platforms and UCY TrustZone-M/TF-M explore acceleration, isolation, attestation and stable PQC APIs.

Secure boot + Firmware Update Over-The-Air → lifecycle agility

CSEM/Valeo: secure boot, PQC-authenticated updates and protected key use & side-channel resilience for embedded crypto.



SELLABLE SILICON HOOKS → device identity / PQC acceleration / enclave & attestation / secure lifecycle

Crypto-agility + programmable networking: update the stack, not the silicon

FOCAL links adaptable accelerator IP to stable software interfaces and programmable I/O
→ allowing algorithms, keys and policies to evolve across the product lifecycle.

Reusable kernels	Adaptable accelerator	Stable crypto interface	Programmable data plane	PQC-aware protocols
NTT / ECC SHA-2/3, field ops	reconfigurable coprocessor vector + hash engine	PSA API / TEE/WASI policy + key control	eBPF/XDP SmartNIC / DPU	QUIC / TLS hybrid migration

CURRENT FOCAL BUILD

- Reconfigurable coprocessor
- SQISign edge accelerator
- Vector/hash acceleration

LIVE CRYPTO CONTROL

- PSA / TEE interfaces,
- hybrid credentials,
- key rotation and secure update
- no platform replacement

NETWORK OFFLOAD

- I/O adjacent PQC validation
- Programmable dataplane
- SmartNIC/DPU-oriented

reusable IP + stable APIs + programmable offload
=
a quantum-safe platform that can keep changing after deployment.

FOCAL “light” and “heavy” semiconductor Proof-of-Concepts (PoCs)

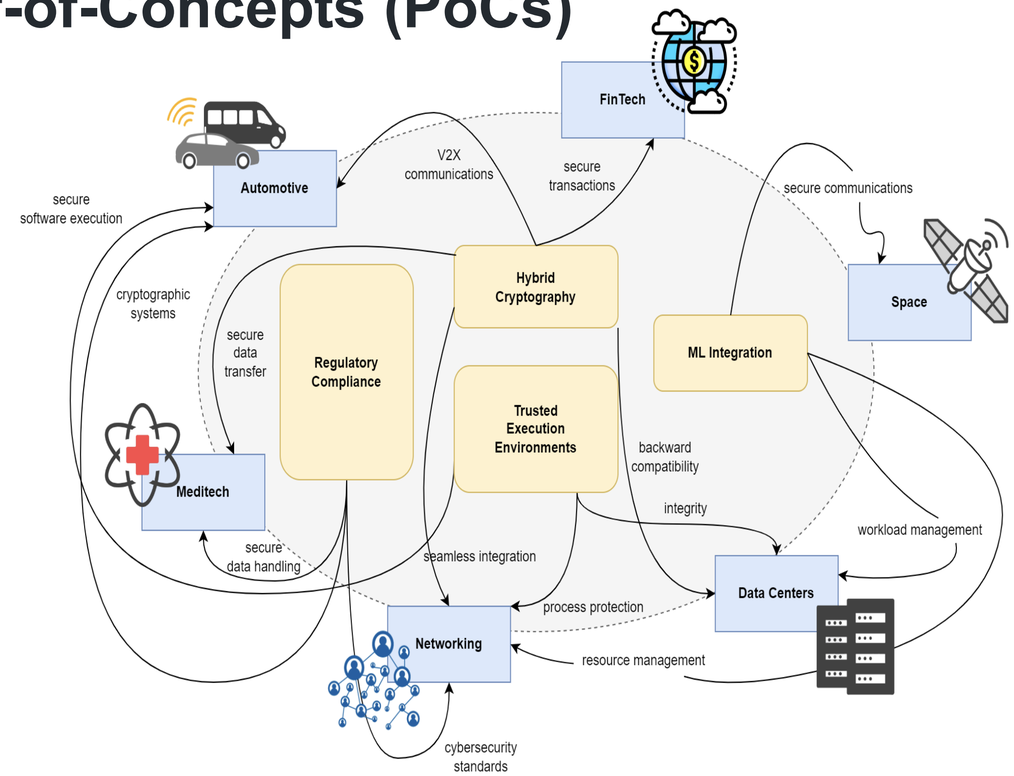
“Light”

Space

- Physical layer security
- Ground station network cryptoagility.
- Application-driven QKD + PQC (end-to-end)

Fintech

- Digital signature and key encapsulation for sensitive financial transactions.
- eID and eWallet applications



“Heavy”

Automotive

- PQC secure boot/update, HSM/TEE and vehicle-to-backend crypto.
- **Chip hook:** secure lifecycle + hardened crypto.

Data centres & Networking

- PQC attestation, firmware signing and East–West / North–South protection.
- **Chip hook:** accelerator + DPU/TEE.

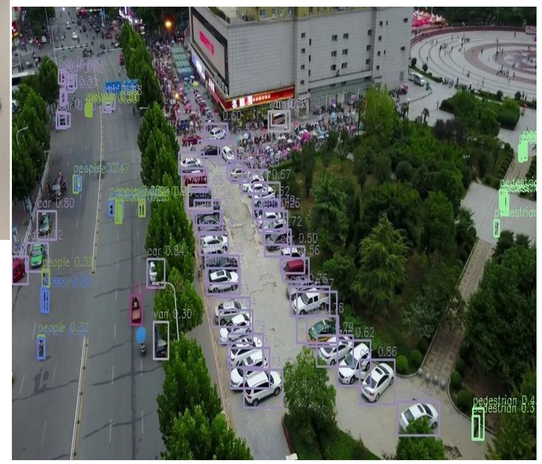
Medical IoT

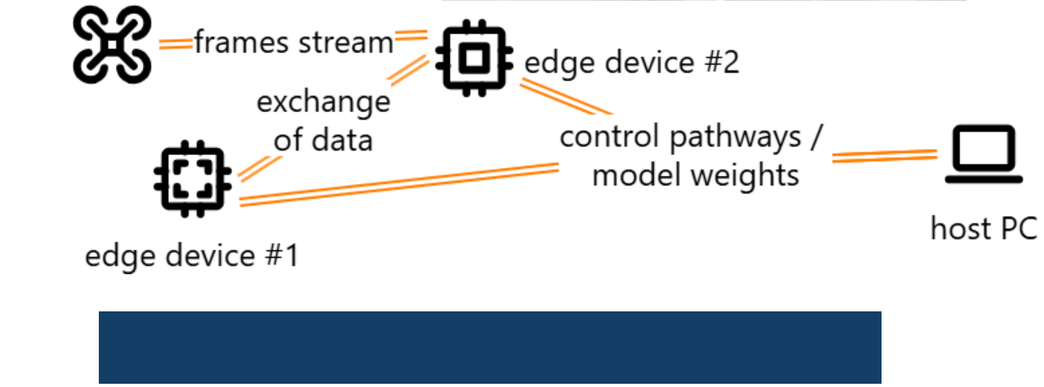
- Hardware-protected keys, onboarding, PQC links and long-lived updates.
- **Chip hook:** low-power trust + agility.

Across the PoCs: hardware trust + crypto-agility + measurable application performance.

Peripheral / experimental use case: making PQC practical at the edge (Surveillance)







Resource identification & optimisation

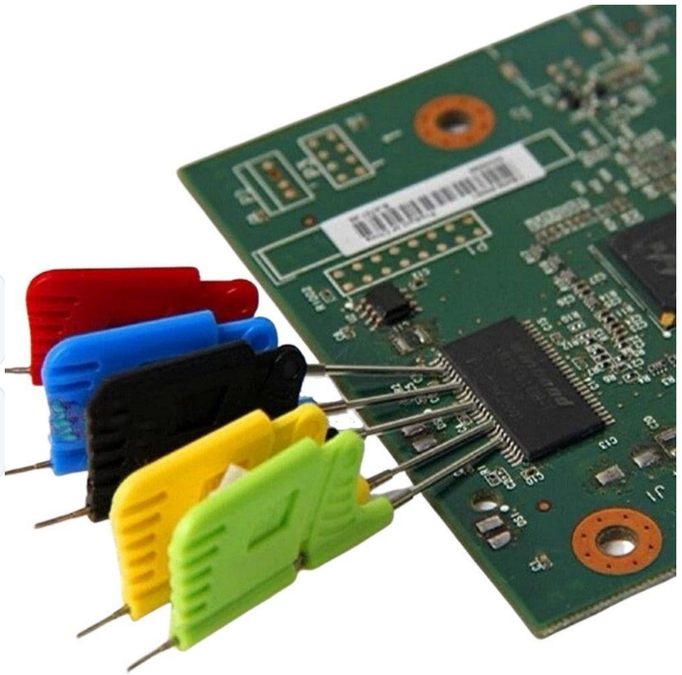
- Heterogeneous targets — FPGA, bare-metal MCU, RTOS and virtualised nodes.
- Measure the real PQC tax — CPU, RAM, energy and network overhead.
- Feed evidence into resource-aware scheduling and crypto-agile deployment decisions.

CPU	RAM	**Energy**
cycles / load	**footprint**	**per secure task**

FOCAL → product hooks for the semiconductor ecosystem

Five product-facing hooks from FOCAL

ACCELERATOR IP	reusable NTT/ECC, hash and PQC kernels
ROOT OF TRUST	PUF/TRNG, secure storage and device identity
TEE + ATTESTATION	protected keys & quantum-safe workload trust
SECURE LIFECYCLE	boot, FUOTA, rotation and hybrid migration
CRYPTO-AWARE I/O	eBPF/XDP + SmartNIC/DPU offload



Evidence that matters to chip designers: area, power, memory, latency, entropy, jitter, side-channel resilience

FOCAL's "sell": reusable IP + APIs + benchmarks + deployment evidence.

semi™ | SEMICON® EUROPA

FOCAL

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

European Commission

Thank you!

FOCAL | Building practical quantum-safe systems from silicon to cloud

TRANSFORM TOMORROW