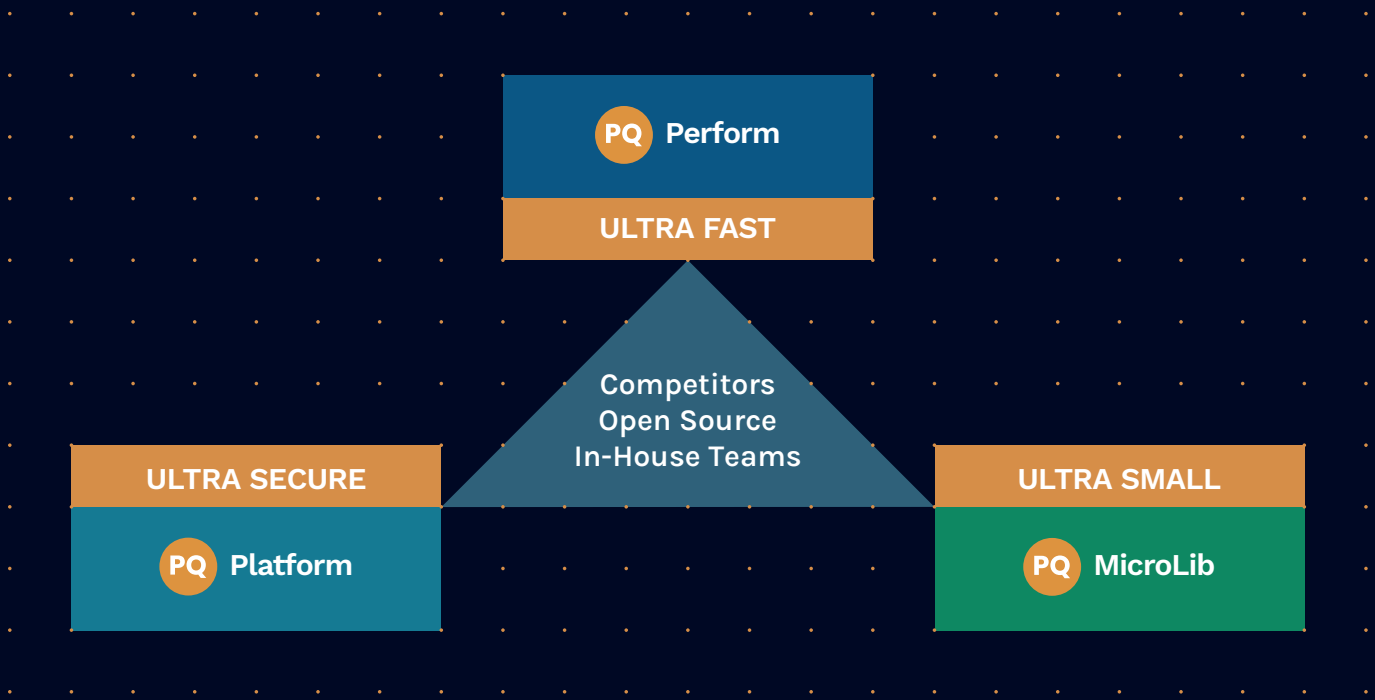
PQ SHIELD

Highlights: Deeply specialized implementations of PQC

PQC is a fundamental change of the maths behind modern cryptography. This means the way in which it's implemented becomes increasingly important. It's even more acute at the extremes of fast-performance, high-security, and low-footprint

PQShield's deep knowledge of the new PQC standards and the maths, our patents, protocols and security techniques, enables us to move way beyond the competition, in-house development and open-source, and it means we can deliver high-quality products to address these optimization problems head-on.

This allows vendors to reduce time-to-market and build PQC into both green and brownfield products.



Ultra Secure
PQPlatform-TrustSys

Example: Post-quantum platform security for Greenfield space applications ASIC

Building an ASIC for long lifecycle products including space applications requires the highest levels of PQC security, Side Channel and Fault Injection protection provided by PQPlatform

Ultra Fast
PQPerform-Inferno

Example: Accelerated Quantum-secure TLS for networking hardware

Delivering high-performance PQC at the core of the network leverages PQPerform to deeply accelerate existing and new FPGA applications, and optimise power consumption

Ultra Small
PQMicroLib-Core

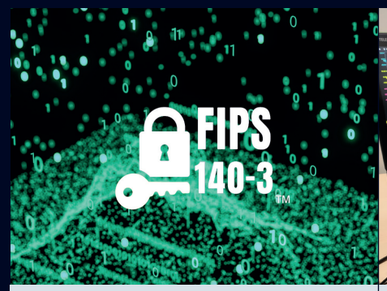
Example: Bare-metal post-quantum security with minimal RAM footprint and optional DPA protection

Existing solutions like smart meters, often have very constrained memory but can be upgraded to PQC using PQMicroLib in < 5 KB RAM in certain configurations

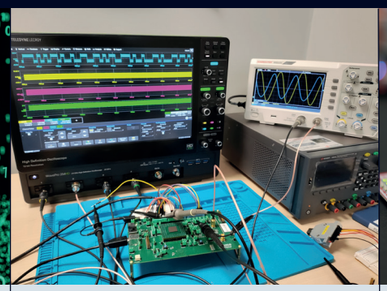
PQShield: global post-quantum cryptography experts

PQShield are world-leaders in PQC standards, with a team of 90+ throughout the EU, UK, US, and Japan.

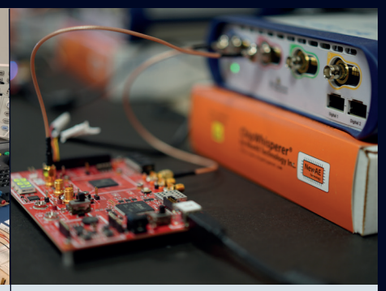
- 50+ Specialist PQC Cryptographers and Engineers
- Co-authors of the first NIST international PQC standards
- Significant contributors to RISC-V, IETF, ETSI, GlobalPlatform, WEF, GSMA, Mitre PQCC and NCCoE... and many more
- Leading authority on real-world PQC implementation, including Side Channel and Fault Attack resistance, FIPS 140-3 certification
- 100+ peer reviewed papers and 40+ patents to date
- High quality, certifiable quantum-safe cryptography in software IP and hardware IP for the global secure products supply chain
- Supporting NIST ML-KEM (FIPS-203), ML-DSA (FIPS-204), SLH-DSA (FIPS-205), LMS & XMSS (SP800-208)



Highly Compliant
All our products are FIPS 140-3 CAVP compliant, plus a number are already certified to CAVP and CMVP.



First Time Right & Crypto Agile
We have the first NIST-compliant PQC in silicon, via our own test chip, proving our IP's quality and crypto agility.



Expert Security Lab
Global standard security levels, including Cloud, Edge, Lab and Government grade options, validated in our own expert lab.

UltraPQ-Suite: Mature PQC in Software, FPGA and ASIC

PQShield provides a powerful range of IP implementations for hardware, software and applications, designed to fit the ultra-small, ultra-fast and ultra-secure use cases you need for your PQC migration.

Family	Product	Description
Embedded Software IP	MicroLib Core	Optimizable baremetal PQC library in < 5 KB RAM with option to include DPA protection
System Level Software IP	CryptoLib Core	Highly configurable SW PQC Library for Classical, PQC and PQ/T Hybrid on Linux, Windows and Mac OS
	CryptoLib SDK	Core + OpenSSL 3.x Provider for ease of integration
Platform Security Hardware IP	Platform AES	AES accelerator with SCA
	Platform CoPro	Highly configurable HW PQC acceleration for existing subsystems, from Hash only to PQ/T Hybrid, with SCA and FIA
	Platform TrustSys	Highly configurable autonomous HW PQC acceleration with RISC-V processor for full CPU offload, configurable as a Sub-System or Full Root of Trust, with SCA and FIA
Performance Hardware IP	Perform Flare	Single instance HW Lattice PQC ultra accelerator as an AXI subordinate
	Perform Inferno	Highly configurable HW Lattice PQC ultra acceleration in AXI4 & PCIe based systems - from Core only to Multi-instance Manager with Queuing or Streaming
	Perform Flex	Inferno + RISC-V processor for enhanced crypto-agility

Shielded

The last line of cyber defense

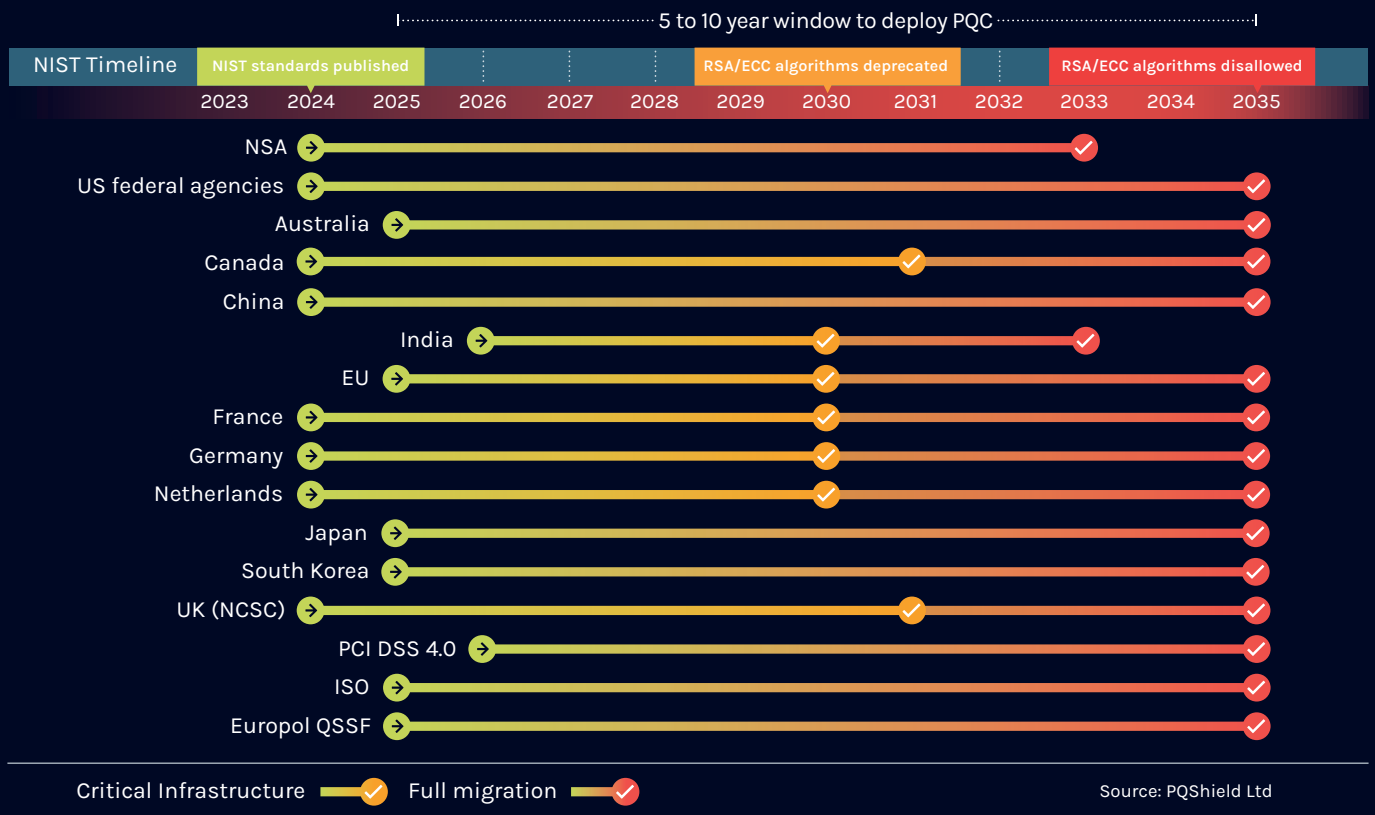
Check out your definitive guide to navigating the quantum era of cybersecurity. Available on all major podcast platforms or follow the QR code link.

PQ SHIELD

Why Now? A five to ten year window to migrate to PQC

Within the next decade, quantum computing will be sufficiently capable of breaking traditional cryptography methods; it's important to be ready for the impact. That's why post-quantum cryptography (PQC) matters - it's the field of new algorithms that use different mathematical techniques to protect against quantum computers.

What's more, the world is adapting quickly for the quantum age. Governments, industries and standards organizations around the world are already putting policy and processes in place to make sure that the equipment we build today is protected tomorrow.



Source: PQShield Ltd

Get in Touch: See how we can help you in your region.
contact@pqshield.com | **www.pqshield.com**

PEERS QUALITY ASSURANCE LTD UKAS MANAGEMENT SYSTEMS
ISO/IEC 27001:2022 9940

PEERS QUALITY ASSURANCE LTD UKAS MANAGEMENT SYSTEMS
ISO 9001:2015 9940

Assured Service Provider
National Cyber Security Centre
Consultancy: Post-Quantum Cryptography (Discovery and Migration Planning)

Assured Service Provider
National Cyber Security Centre
Consultancy: Post-Quantum Cryptography (Advice)