With Cryptography, if you don't keep ahead, you're falling behind

PQSHIELD

Think openly, build securely

The Quantum Threat

It's no secret that quantum computers pose a significant threat to information security. That can sound daunting, but it needn't be – there are steps you can take now to protect your organization in the long-term.

Both the NCSC (the UK National Cyber Security Centre) and the NSA (the US National Security Agency) agree that the best mitigation against this threat is post-quantum cryptography.

In fact, the NIST (US National Institute of Standards and Technology) Post-Quantum Cryptography Standardization Project is now in its final stages, with official standards expected to be announced in December 2021.

For more on the Quantum Threat

See our comprehensive and acclaimed white paper series at pqshield.com/quantum-threat

Risk Assessment and Solution Design

We all know that the software used to run the world is vulnerable to hackers, back doors and bad actors. Even worse, with quantum attacks, every bit and byte of data from any organisation, individual or government is left exposed to rapid decryption and widespread dispersal. The products manufactured today have hardware that's built to last, but security that is not.

We can collectively change this. As a cryptography and security solutions supplier, PQShield aims to work together with Critical Infrastructure, OEM and IoT partners, and a host of other sectors to make this security upgrade smooth and professional.

Discuss

There is a lot of confusion around post-quantum security and the new standards - we're here to guide and talk you through it every step of the way.

Evaluate

Existing projects and infrastructure can be expertly and swiftly evaluated for the quantum risk and the crypto-agility of the underlying architecture.

Design

We deliver an end-to-end solution design that is provably secure, crypto-agile, efficient and compliant with international standards (FIPS, etc.).

Implement

Working standalone or as part of your wider team, we have the resources and expertise to securely implement and deploy entire solutions for you, end-to-end.

Advise

Collectively, we've spent decades developing the research, designing the solutions and setting the standards in the field.

Our team is here to help you think openly, build securely.

PQSoC

Post-quantum Cryptography Hardware for Embedded Devices

- End-to-end verifiable hardware SoC design with multiple co-processors for classical and PQC.
- 1st delivery of classical hardware-based Entropy Source based on our RISC-V spec.

PQSlib

Post-quantum Cryptography Firmware for Embedded Devices

- Lightweight PQC libraries for IoT and Embedded Devices.
- Portable code for use with any IoT platform.

PQSDK

Post-quantum Cryptographic SDK for Mobile and Server Technologies

- PQC libraries with Engines to update OpenSSL and APIs for PKI, TLS, VPN (IPSec and OpenVPN), and TEEs.
- FIPS certified hybrid solutions by the end of the year.

PQE2E

Post-quantum Encryption Solution for Messaging Platforms and Apps

- An SDK for enabling end-to-end encrypted messaging solutions using PQ algorithms.
- Uses a new, provably secure, Signal-derived protocol.

About PQShield

Our world-class researchers and engineers are co-authors of multiple finalist algorithms within the NIST Post-Quantum Cryptography Standardisation Process, which aims to define standards for the next generation of public-key cryptography.

Defining post-quantum cryptography, leading projects for the Crypto Task Group at RISC-V (e.g. TRNG, AES-ISE, etc.) and contributing to the Internet Engineering Task Force (IETF) – that's how familiar we are with cryptography standards, and that's how extensive our expertise is in the quantum-safe cryptography solutions domain.

We are creating the global standards and core technologies to power the security layer of the world's leading organisations.

We started out life as a modest Oxford University spin-out but our team is now made up of many world class researchers, mathematicians and engineers – giving us the highest concentration of cryptography PhDs in the industry.

Collectively, we've spent decades developing the research, designing the solutions and setting the standards in the field, so we are in a perfect position to help you with products, risk assessment and solution design.

Our goal is to bridge the gap between academic theory and commercial practice, between openness and security, between the ideal world and the real world.

Start a conversation today!

pqshield.com/contact us

PQ SHIELD

Think openly, build securely