Post-Quantum Cryptography Experts

› Hardware › Software › Services › Content

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.

Organisations like 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 being announced imminently in 2022.

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

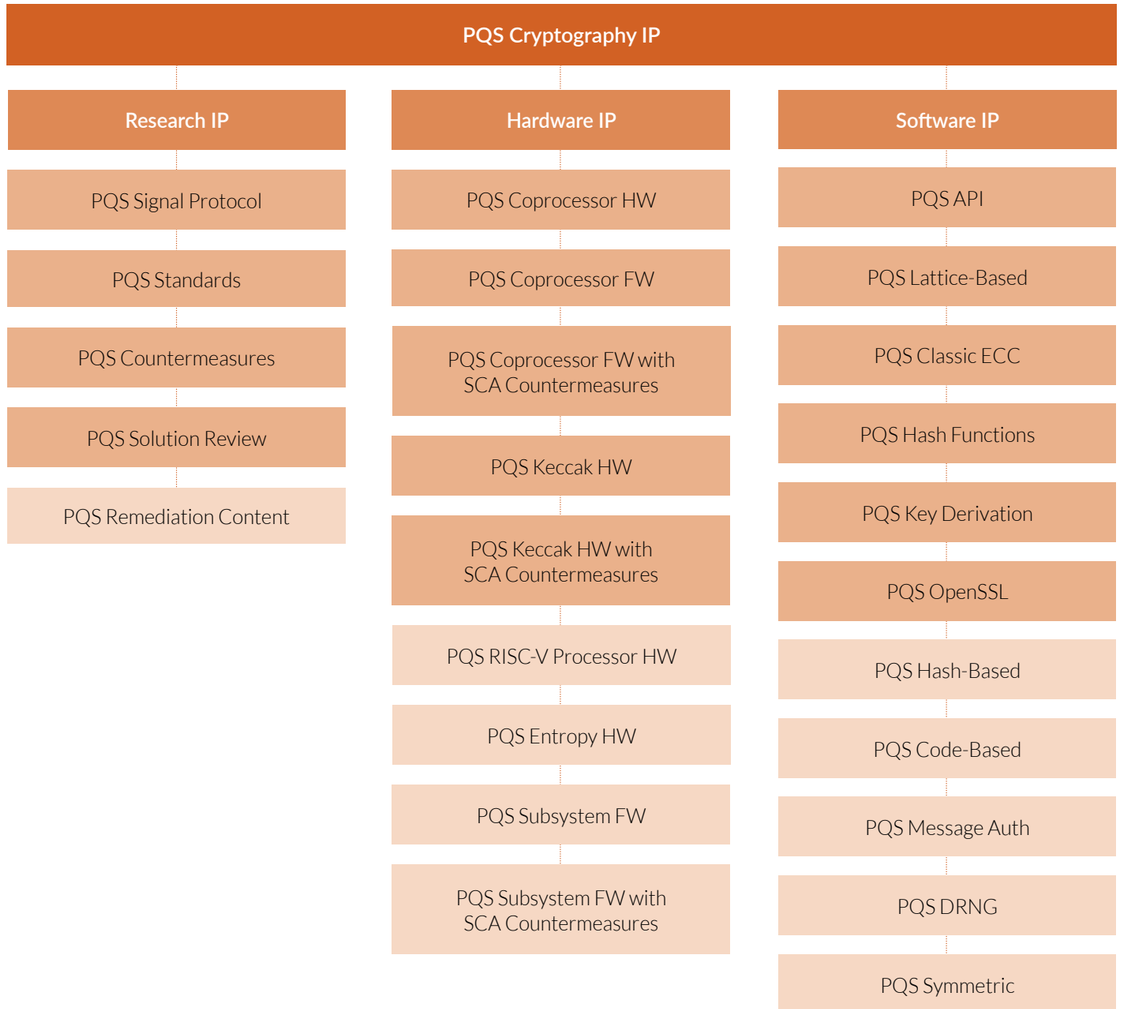
Collectively, we've spent decades developing the research, designing the solutions and setting the standards in the field.

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

Hardware and Software products today, that protect against tomorrow

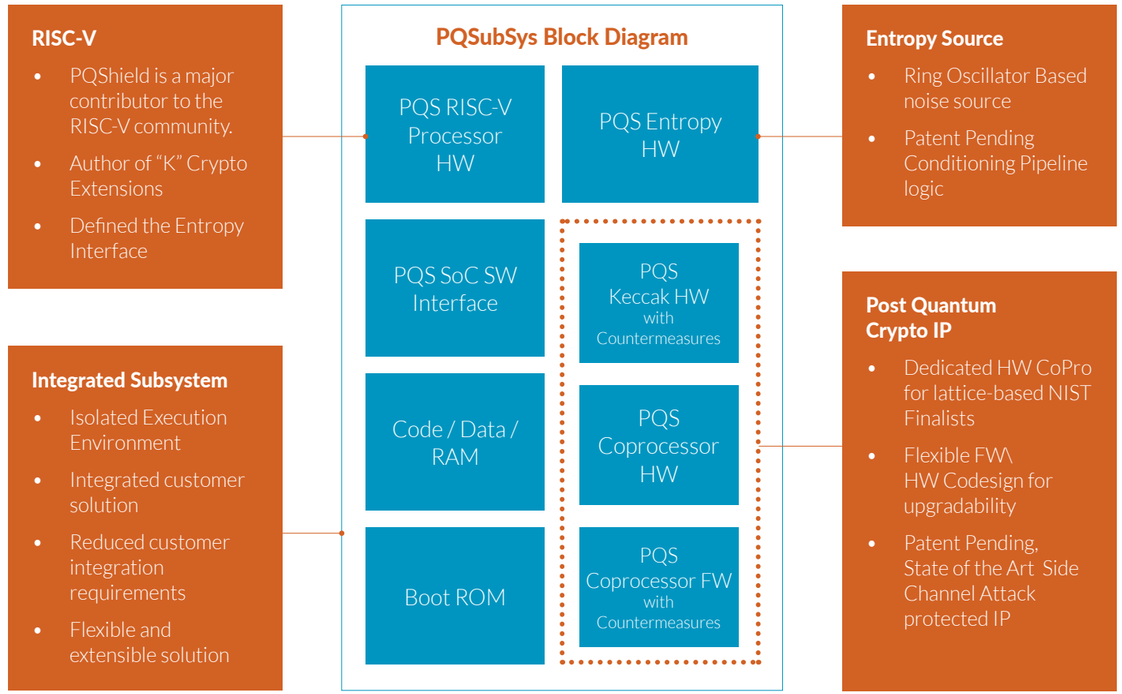
Comprehensive Cryptographic IP

The expert team at PQShield have delivered significant research that has not only fed into the emerging global standards for Post-Quantum Cryptography, but also into our own solutions and product portfolio.



These Research, Hardware and Software IPs can be combined into use case specific implementations for chips, applications or the cloud. Just a couple of examples are shown on the next page:

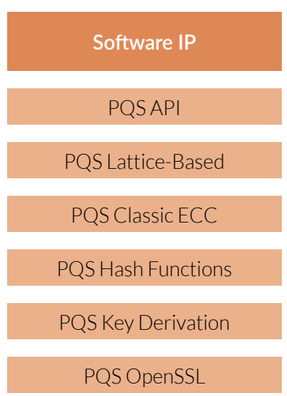
Example Post-Quantum Hardware IP: PQSubSys



Example FIPS 140-3 Ready Software IP: PQCryptoLib

Our hybrid cryptographic library, PQCryptoLib, was the first ever submitted to be validated by the NIST Cryptographic Module Validation Program for FIPS 140-3, the mandatory standard for the protection of sensitive or valuable data within federal systems in the US and Canada.

The PQCryptoLib is a library of modern cryptographic primitives that is designed with crypto-agility in mind to help companies transition smoothly and securely to the quantum-era, e.g., it provides support for classical and hybrid key derivation and for implementation within the TLS key schedule, supporting multiple Post-Quantum NIST finalist algorithms as well as many classical schemes.



PQShield's Expertise

PQShield is a cybersecurity company specializing in post-quantum cryptography, protecting data from today's attacks while readying organizations for the threat landscape of tomorrow. We are the only cybersecurity company that can demonstrate quantum-safe cryptography on chips, in applications, and in the cloud.

Headquartered in the UK, with teams in the United States, France, Belgium, the Netherlands and Japan, our quantum-secure cryptographic solutions work with companies' legacy systems to protect devices and sensitive data now and for years to come.

We started out life as a modest Oxford University spin-out 4 years ago, but the company has grown rapidly to drive global awareness of the quantum threat. 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.

PQShield is a leading contributor to the National Institute of Standards and Technology (NIST) post-quantum cryptography standardization project, having co-authored two of the seven algorithms (NTRU and FALCON), and advised extensively on all other schemes.

Team PQShield have also contributed multiple cryptographic extensions to RISC-V, the open standard instruction set architecture (ISA) that is rapidly gaining traction from proprietary competitors such as ARM and Intel, alongside working with many other organisations like the World Economic Forum and GlobalPlatform, to advise and define their own positions.

In short, we are creating the global standards and core technologies to power the security layer of the world's leading organisations.

PQSHIELD

Think openly, build securely

Start a conversation today! pqshield.com/contact us