PQSHIELD

Post-Quantum Cryptography for Defense and Governmental Applications:

Overview and Use Cases

Protecting the Military against the Quantum Threat to Today's Cryptography

Quantum computers have the potential to break many of the currently used cryptographic schemes, such as RSA and ECC, due to their ability to efficiently solve certain mathematical problems. Post-quantum cryptography (PQC) is a class of cryptographic algorithms that remain secure even in the presence of powerful quantum computers, thus ensuring the continued security of sensitive information in the future.

PQC solutions can help upgrade hardware (such as vehicles, sensors and hardware security modules) and software (such as public key infrastructure, TLS and virtual private networks) to become crypto-agile and quantum-resistant. Classified data held by defense and aerospace organizations can have a long shelf-life, and even now is at risk of interception and future decryption.

PQC is fully available technology that is deployable today in the existing defense infrastructure, on today's computers and over today's network, upgrading it to be quantum-secure at low risk and low cost. In simple terms, all that is necessary is to replace the old cryptography software with new PQC software.

It offers both confidentiality by unbreakable encryption as well as authenticity using unforgeable digital signatures.

With a 70+ strong team in the UK, US, EU and Japan, including 25+ Specialist PQC Cryptographers and 25+ Hardware & Software Engineers, UK-based PQShield Ltd. is the world leader in research and implementation of Post Quantum Cryptography.

Post-Quantum Cryptography Solutions from PQShield

PQShield offers Software Libraries for application/system developers, as well as Hardware IP for FPGAs, SoCs or ASICs. The PQC Software Libraries are available for standard processors (X86, ARM) as well as for memory-constrained embedded systems and can be deployed on most computer systems. The Hardware IP ranges from math accelerators to completely autonomous crypto subsystems that can easily be integrated into FPGAs or new processor designs.

Our products are optimized for top-level security with high efficiency and performance. They offer advanced security features like configurable Side Channel Attack (SCA) Resilience and optional Fault Injection Resilience. FIPS 140-3 certification is already in progress, with more certifications coming.

They support post-quantum, classical and hybrid cryptography and cover commercial cryptography standards including the NIST PQC standard. With our leading cryptography expertise, we can also offer Sovereign "Suite A" implementations on request.

Defense Use Case Examples

Anonymized Use Case:
Quantum-secure C4 for next generation battlefield systems

A major defense supplier required a partner who could help them design the next generation of cryptographic deployments for mission-critical technology. The IRAD projects were focused on the impact of PQC to military communication systems and analysis of specific comms use cases, including SCA and Fault Attack considerations. PQShield supplied deep-dive research with design methodology, recommendations and solution proposals.

Status: Two projects completed, implementation and further projects following

Anonymized Use Case:
Post-quantum secure boot

Ruggedized Single Board Computer for military applications required Side-Channel-Attack-protected PQC Secure Boot, that ensures that the computer only executes the authenticated original software: PQShield's highly-secure Hardware IP is deployed on the Single-Board Computer's FPGA.

Status: Integration underway

Use Case: End-to-end encryption for classified information sharing

PQShield supplied its FIPS 140-3 ready PQC software library for integration with MindLink to provide a Zero-Trust, end-to-end encrypted solution to enable secure sharing of classified information in a post-quantum world.

Status: Integration underway (via AWS EU Defense Accelerator)

Use Case: PONE Biometrics
Biometric user authentication using FIDO2 on ARM Cortex M4

FIDO2 enables passwordless user authentication between client app and server. FIDO2 uses ECC signatures to authenticate a user at the server. ECC signatures are supplemented with PQC signatures, using PQShield's PQC software library.

Status: Integration completed

PQ SHIELD

Ready to learn more?
Get in touch: contact@pqshield.com
www.pqshield.com

Products | Publications | Careers