FortifyIQ

Interview:

Securing the Post-Quantum Era

A Conversation with FortifyIQ's

Yaacov Belenky

Chief Innovation Officer

The industry is rapidly moving toward post-quantum cryptography (PQC). Why does it need protection if it's supposed to be "quantum-safe"?

That's a critical question. PQC algorithms such as ML-KEM (Kyber) and ML-DSA (Dilithium), now standardized by NIST in FIPS 203 and FIPS 204, are designed to resist mathematical attacks by quantum computers. But their implementations are highly vulnerable to physical attacks, particularly side-channel and fault-injection attacks. In fact, several masking-based PQC implementations have been broken in academia, some with only a single trace. These are not hypothetical risks; they're practical, exploitable vulnerabilities.

How urgent is this problem?

Very. Adversaries are already harvesting encrypted data today to decrypt later, once quantum computers become capable of breaking RSA and ECC. That makes protecting PQC not just a future requirement but an immediate one, especially for high-assurance systems, critical infrastructure, and connected devices with long operational lifetimes. Regulators are also catching up quickly: NIST, ETSI, and national certification bodies are seriously considering this topic and are expected to update the regulations/standards to mandate SCA/FIA protection of PQC implementations, incorporating side-channel and fault-injection requirements into post-quantum compliance.

What makes FortifyIQ's approach different from masking-based protections?

We use an algorithmic hardening approach that operates at the mathematical level of the implementation, not just at the masking level. It's the same family of techniques we've validated for our AES and HMAC SHA-2 cores, which passed AVA.VAN.5 evaluation by a Common Criteria lab. The protection is intrinsic to the design and validated as robust against side-channel and fault-injection attacks. Because of this approach, our PQC solutions achieve resilience comparable to hardened hardware, without the large overhead typically associated with masking.

Let's talk about performance. What's the impact of these protections?

In software, our SCA/FIA-resistant PQC implementations are on par with the performance of naïve PQC implementations, with the only overhead in code size (under 10 percent), whereas our data RAM requirement is lower than that of naïve PQC.

In hardware, we can match the performance of naive PQC implementations. Alternatively, for resource-constrained devices, we can keep the area comparable to naive PQC implementations. The implementation is fully soft IP, and the integration is identical to any standard macro, with no special constraints or tool requirements.

You mentioned both hardware and software implementations. How are they deployed?

Our FortiPQC suite includes OTA (over-the-air) deployable software libraries, hardware IP cores, and hybrid CryptoBoxes that combine both PQC and traditional cryptography - AES, HMAC SHA2, RSA, and ECC, all hardened against side-channel and fault-injection attacks. The hybrids are particularly important because we're in a long transition period: many deployed devices will still require RSA or ECC for compatibility. Our CryptoBoxes and Roots of Trust provide that dual capability efficiently, without duplication of logic or power penalties. Our asymmetric cryptography, including the PQC, is FOTA (firmware-over-the-air) updatable.

Are these implementations updatable?

Yes. Both our software and our asymmetric cryptography, RSA/ECC and PQC in hardware, are designed for secure OTA (Over-The-Air) and FOTA (Firmware-OTA) updates. That's essential for PQC because new attacks are likely to emerge in this new technology.

Can FortifyIQ tailor its hardware and software cryptography IPs to specific customer requirements?

Yes. FortifyIQ works like a security boutique. All our hardware IP, software libraries, and hybrid CryptoBoxes or Roots of Trust can be customized throughout the project, right up to tape-out, to match specific device constraints, performance goals, or certification needs.

Our customers can balance performance, area, and power as they see fit. They can include only the cryptographic blocks they need (AES, HMAC-SHA2, PKA, or PQC) or combine them with our software libraries, allowing for seamless switching between hardware and software under a unified architecture. This flexibility is especially useful during transition periods.

And importantly, every version maintains certifiable protection against side-channel and fault-injection attacks. This approach ensures that each system, from small IoT devices to high-performance cloud or edge platforms, receives optimized, high-assurance cryptography tailored to its environment.

What types of customers or systems is this designed for?

It spans everything from embedded controllers and IoT devices to cloud and data-center accelerators. The same FortiPQC architecture scales with power and performance targets, from microcontroller-class to multi-gigabit throughput. Our Roots of Trust even supports on-the-fly encryption with full SCA/FIA resistance, which is increasingly demanded for chiplet-based architectures and heterogeneous systems.

What's your view on the bigger picture? Where is PQC protection headed?

Post-quantum migration is unavoidable, but secure post-quantum deployment isn't automatic. Protecting PQC against physical attacks is as fundamental as adopting the algorithms themselves.

Can you summarize FortifyIQ's overall goal with FortiPQC?

Our goal with FortiPQC, across software, hardware, and hybrid systems, is to make post-quantum protection intrinsic, certifiable, and practical for every device class. We achieve this by applying algorithmic protections that leave our protected devices to rival the PPA (Power-Performance-Area) of unprotected implementations, even in the most constrained configurations, only doubling latency without power or area penalties. FortiPQC delivers high-assurance post-quantum cryptography ready for real-world deployment.

What standards and certifications does FortiPQC address?

FortiPQC aligns with FIPS 203, 204, 205, NIST SP 800-208, and ETSI TS 103 619, and is engineered for FIPS 140-3 Level 4, Common Criteria AVA.VAN.5, and SESIP Level 5. Every implementation, hardware or software, is designed for certifiability from the start.

About FortifyIQ

FortifyIQ engineers certifiable cryptographic IP cores, software libraries, and roots of trust with traditional and post-quantum algorithms, all hardened against side-channel and fault injection attacks, without compromising performance, area, or energy efficiency. Our solutions are foundry- and platform-agnostic, integrating securely across a wide spectrum, from smart cards and IoT devices to AI accelerators and cloud systems.

Backed by a strong portfolio of granted and pending patents, deep cryptographic research and formal and practical security proofs, FortifyIQ's IP is developed and validated using our own pre- and post-silicon EDA tools, enabling systematic evaluation of physical attack resilience.

FortifyIQ delivers advanced cryptography that is certifiable, reliable, and built to meet the challenges of high-assurance, real-world applications.

FortifyIQ

Media Contact:

Olivier Debelleix

VP of Business Development

info@fortifyiq.com