WHITEPAPER Mar 1, 2024

PQC
as It Stands in Industry

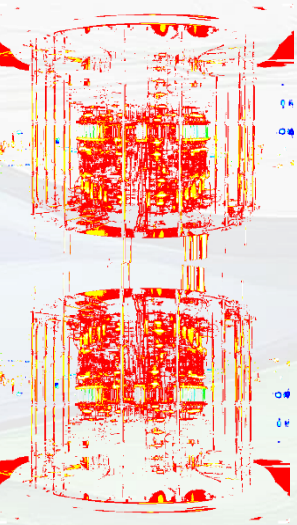
The timeframe for quantum computers capable of breaking standard cryptography is uncertain. IBM aims for a quantum computing inflection point by 2029, while QuEra plans a 10,000-qubit system by 2026. Despite this, bad actors are already harvesting encrypted data for future decryption, known as HNDL attacks, without relying on quantum computers.

PQC Industry Updates

Ericsson gives PQC progress report

at Mobile World Congress. Telecom operators are adopting post-quantum cryptography (PQC) to secure their networks against future threats from quantum computers. Key challenges include getting leadership buy-in, creating a migration strategy, and hardware limitations. Software updates are easier than hardware upgrades, which may require modernization.

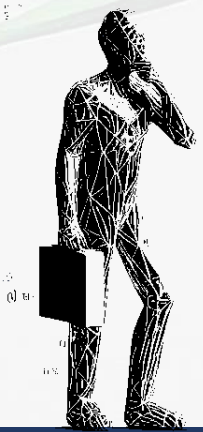
Ericsson's **Taylor Hartley** role has seen her driving executive engagement to get the C-suite on board with the measures they need to take. “But hardware lacks the crypto agility software has. You won’t have to uplift all your hardware, some of it you can patch once or twice. We call this crypto flexible rather than agile. But the reality is there will have to be an uplift and there will have to be modernization that happens to some hardware, and I think that might be the biggest challenge so far.”



Post-Quantum Cryptography Alliance

The Linux Foundation launched the PQCA to tackle security risks from quantum computers. This industry-wide effort (including Google and IBM) aims to develop secure software for new and existing encryption methods. Fearing future threats, the PQCA will create new tools and collaborate with projects like Open Quantum Safe. Industry leaders emphasize the importance of PQCA for providing developers with secure cryptography solutions. Timely action is crucial to safeguard our digital future and national security.

Post-quantum cryptography migration will be complicated



UK's NCSC warns that transitioning to post-quantum cryptography is complex. Beyond math, critical infrastructure systems may struggle with resource-heavy software. Peter Shor's 1994 algorithm challenges traditional public-key security assumptions.

NCSC notes current limitations of quantum computing but warns of future risks. Today's machines have high error rates, but potential for lower errors in the future. Current data could be vulnerable to decryption by future quantum computers. NCSC notes potential high cost for attackers to exploit old data. CRQC threat relevant for organizations with valuable data. Efforts underway for quantum-resistant cryptography like Google's Dilithium standard. PQC development accelerated since 2016 when NIST began seeking feedback. However, transitioning to PQC involves more than adopting new algorithms. Protocols and services must be re-engineered. Transitioning major internet services to PQC is expected to be easier, while legacy protocols in critical infrastructure pose a challenge due to resource demands. Owners must plan for transition during technology refresh cycles.

Apple is future-proofing iMessage

Apple introduced PQ3, a major cryptographic security upgrade for iMessage in iOS 17.4 on Feb. 21. This makes Apple one of the few providers offering post-quantum cryptography. While Signal previously launched quantum-resistant encryption in September 2023, Apple claims to be the first to achieve "level 3" encryption.

Post-quantum messaging involves encrypting messages to withstand potential future threats from quantum computers. Apple's iMessage originally used RSA encryption but switched to Elliptic Curve cryptography in 2019. Currently, breaking this encryption is difficult, but quantum computing poses a potential threat. While no quantum computers can currently break this encryption, preparation is underway. Developing post-quantum cryptography ensures data security for organizations against future threats.

PQC Market Is Expected To Grow At A CAGR Of 19.3% During Forecast Period 2023-2029

The Quantum Cryptography Market Report offers a comprehensive analysis of the global quantum cryptography market, covering key trends, growth drivers, challenges, and opportunities. It examines various market segments such as quantum key distribution, generation, and management, projecting the market's trajectory over the forecast period. The report employs a robust research methodology combining primary interviews with industry experts and stakeholders, along with secondary research methods to gather relevant data and insights.

Quantum Cryptography Market Dynamics: In the current technological landscape, digitalization offers opportunities for optimization across industries. However, the rise in connected devices has led to increased complexity in cyber risk management and a surge in global cyber threats. Nations like the United States, Turkey, Brazil, China, Pakistan, India, and Europe are particularly targeted. To address these threats, there's a growing adoption of quantum cryptography for enhanced security measures.

Quantum Cryptography Market Regional Insight: North America dominates the market with a 48.6% share in 2022. The region's market growth is driven by increasing cyber-attacks, particularly in countries like Canada and Mexico. The extensive use of encrypted applications in the US, coupled with the complexity of IT management and rising demand for data privacy, further fuels market growth. The United States stands out as a highly lucrative market due to its rapid technological adoption and digitization.

UK NCSC issues new guidance on post-quantum cryptography migration

John H, head of crypt research at the NCSC, underscores the complexity of transitioning to PQC, noting the need to overhaul protocols and services due to increased demands on devices and networks. While upgrading internet services may be manageable, transitioning legacy and sector-specific protocols, especially in critical infrastructure, presents additional challenges such as cryptography on resource-constrained device.

The NCSC outlines that PQ/T hybrid schemes, combining post-quantum and traditional cryptography, may incur higher complexity and costs but can be necessary for reasons like interoperability or security; It recommends using them temporarily with a flexible framework for easy transition to PQC-only systems later, urging careful consideration of factors like system complexity, maintenance costs, and protocol constraints by technical and risk owners.

KyberSlash Cryptography Flaw

On December 30, 2023, researchers disclosed the KyberSlash vulnerability affecting implementations of Kyber, a NIST-selected post-quantum cryptography algorithm. Dubbed KyberSlash, this timing vulnerability could lead to private key compromise, echoing previous issues with NIST PQC candidates like SIKE. Joey Lupo, product security architect at QuSecure, emphasized the significance of crypto agility for swift encryption algorithm transitions post-cracking. However, he noted its limitations in safeguarding already stolen IP through 'harvest now, decrypt later' campaigns.

The transition to Post-Quantum Cryptography (PQC) in the next 5 years is critical. In the face of quantum storms, our encryption sails must be woven anew.

Ji-Won (지원)