UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Ingeniería

https://revistas.udistrital.edu.co/index.php/reving/issue/view/1350

DOI: https://doi.org/10.14483/23448393.25956



Editorial

Information Security in the Quantum Eraç

Waldimar Alexander Amaya Ocampo[1]

[1]Quside Technologies S.L, Barcelona, Spain.

In a world where data has become an organisation's most valuable asset, information security is no longer a purely technical issue: it is a strategic priority that permeates all businesses, government and defense entities, and other organisations, and that determines both our competitiveness and the trust placed in us by those who work with us.

Yet the threat landscape is changing fast. Quantum computing, once a distant promise confined to research labs, now advances at a pace that forces us to rethink the foundations of modern cryptography. Encryption we consider robust today — protecting everything from corporate communications to critical infrastructure — could become obsolete once a sufficiently powerful quantum computer exists. This scenario, known as "Q-Day," is no longer a remote possibility, but a risk we must start addressing now by migrating toward post-quantum cryptography before the threat materialises.

Faced with this threat, the cybersecurity community has converged on a key concept: crypto-agility. This refers to an organisation's ability to update its cryptographic mechanisms — algorithms, protocols, and keys — quickly and without needing to redesign its systems entirely. More than a specific technology, crypto-agility is a working methodology: designing architectures where encryption is not hardcoded or fixed, but modular and replaceable. In a context where today's secure algorithms may no longer be secure tomorrow, this flexibility becomes a strategic necessity rather than a technical luxury.

Editorial

©THE AUTHORS; REPRODUCTION RIGHT HOLDER UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS.

*Correspondence: wamaya@quside.com

It is precisely within this framework that NIST (the National Institute of Standards and Technology) has played a decisive role. After years of an open, competitive standardisation process, NIST has selected three post-quantum cryptography (PQC) algorithms designed to withstand attacks from both classical and quantum computers. The goal of this initiative is clear and ambitious: to have private companies, public institutions, governments, defense entities, and, ultimately, every actor participating in global communication networks migrate their current cryptographic systems to these new PQC standards before the quantum threat becomes an operational reality.

This migration, however, is not as simple as "swapping one algorithm for another." And this brings us to a point that, in our view, does not receive all the attention it deserves entropy. Every cryptographic protocol rests on two equally important pillars. The first is the algorithm's mathematical complexity. The second, often underestimated, is the quality of the random numbers that feed that algorithm to generate keys, initialization vectors, and other critical parameters. If those random values are predictable, it does not matter how robust the underlying mathematics is: security collapses.

As explored in a recent analysis, the history of cybersecurity is full of breaches caused by poor entropy. In 2008, a flaw in Debian's OpenSSL implementation reduced the effective key space from a 39-digit number down to just 32,767 possible keys, leaving millions of systems exposed for nearly two years. In 2010, Sony reused the same random number in the PlayStation 3's digital signature scheme, allowing attackers to fully extract the private signing key. More recently, and more relevant here, 2024 research showed that even NIST-approved post-quantum algorithms, such as ML-KEM/Kyber, are vulnerable to secret recovery when seeded with low-quality entropy.

This is crucial: migrating to PQC does not eliminate the risk of poor entropy generation. As post-quantum cryptography moves into production, the consequences of unreliable entropy are growing larger, not smaller. Today's systems typically rely on operating-system pseudo-random number generators (PRNGs), seeded from sources such as electronic noise or hardware timing variations. However well designed, these generators can never produce more unpredictability than their seed provides: a weak seed means a weak output. The strategy gaining traction in the most demanding PQC environments combines these generators with external, verifiable entropy sources — such as quantum random number generators (QRNGs) reinforcing security through independent layers of unpredictability, while enabling real-time, local verification that this entropy is genuinely of high quality, rather than simply trusting a static certification.

The lesson is therefore twofold: it is not enough to adopt quantum-resistant algorithms; the randomness feeding them must also be robust, verifiable, and continuously monitored. Crypto-agility should be understood not just as the ability to switch algorithms, but as the ability to guarantee, at every link of the cryptographic chain — including entropy generation — that systems withstand both present-day scrutiny and future threats.

It is tempting to think of "Q-Day" as a distant horizon, a problem for the next generation of security leaders. That perception may be the greatest risk of all. Information encrypted today with vulnerable algorithms can be intercepted and stored now, to be decrypted later once the computational power exists — the well-known "harvest now, decrypt later" strategy. Every day of delay is, quite literally, information that is already compromised, even if we do not yet know it.

The consequences are not abstract. Behind every encrypted database lie medical records, financial data, private communications, and government records. A delayed or poorly executed migration is not merely a technical or compliance issue: it is ultimately a matter of privacy and of the well-being of the people whose information we protect.

As engineers and stewards of our systems' security, adopting crypto-agility, migrating to NIST's PQC algorithms, and ensuring robust, verifiable entropy are not tasks that can wait for a "more convenient moment." That moment is now. Organisations that begin this process today — auditing their cryptographic systems and establishing migration roadmaps — will protect not only their own infrastructure, but also the trust and privacy of everyone who depends on it. Quantum security is not a question of if, but of when.

CC BY NC SA