QUANTUM
THINK TANK

Insight that protects. Foresight that leads

# Quantum-Safe Principles

By Tooba Qasim

January 2026

www.cyberlondon.com | info@cyberlondon.com

## Building a Secure Foundation for the PQC Era

Quantum computing may still feel like "future technology," but the security risks it brings are very real today. Organisations around the world are preparing for a world where quantum computers can break the encryption we rely on and the shift is not just about using new algorithms.
It is about **changing how we think about security itself**.

In this article, we will break down the core *quantum-safe principles* in simple language with just enough technical insight to help you plan effectively. We will also explain why these principles matter long before quantum computers arrive and why organisations must begin adapting now.

## What Does "Quantum-Safe" Actually Mean?

Let's start by clearing up one common misunderstanding.

**Quantum-safe does *not* mean using quantum computers, quantum networks, or quantum magic.**

It simply means:

**Designing systems that stay secure even when powerful quantum computers exist.**

Today's encryption (RSA, ECC) relies on mathematical problems that classical computers struggle with but quantum computers will solve those problems extremely quickly. So becoming quantum-safe is about **protecting data and systems from that future capability**.

Think of it like upgrading a lock on your house because you know that one day, burglars will have a tool that can easily open your current lock. You upgrade *before* the burglars show up, not after.

To move confidently into the post-quantum era, organisations need to understand a set of foundational principles. These principles act like guiding markers, helping teams understand what "quantum-safe" really means in practice. Before selecting algorithms or

upgrading systems, an organisation must understand these principles clearly because they influence every decision that follows.

## Principle 1: Crypto Agility (The Ability to Change Algorithms Easily)

Crypto agility is the cornerstone of every quantum-safe strategy. It refers to the ability to replace cryptographic algorithms without redesigning entire systems or disrupting operations. In many existing environments, cryptography is deeply embedded within applications, network protocols, hardware modules and even business logic. Once embedded, it becomes extremely difficult and expensive to replace. This worked well during the classical era, because algorithms like RSA and elliptic curve cryptography remained stable for decades. However, the post-quantum era will not offer the same comfort.

A quantum-safe organisation must be prepared for cryptographic change. Even though NIST has standardised ML-KEM for encryption and ML-DSA and SLH-DSA for signatures, these algorithms will continue to evolve. Additional schemes may be standardised, parameter sets may be refined, and new vulnerabilities may eventually appear. Crypto agility ensures that organisations can adapt to all of these developments without rewriting thousands of lines of code, replacing costly infrastructure, or creating long service interruptions.

The best way to understand crypto agility is through a simple analogy. Imagine that your home has a door lock, but instead of being bolted into place, the lock is designed so that you can slide it out and replace it at any time. If the manufacturer discovers a flaw, or if a stronger and more secure lock becomes available, you can install it without replacing the entire door. Crypto agility brings this same level of flexibility to digital systems, ensuring that cryptography can evolve without destabilising the environment around it.

The more an organisation embraces crypto agility, the more prepared it becomes for a fast-changing cryptographic landscape. Rather than viewing cryptography as a fixed element that remains unchanged for decades, crypto agility treats it as a dynamic component that can be updated whenever necessary. This mindset shift is essential for long-term security.

## Principle 2: Hybrid Cryptography (Combining Classical and Post-Quantum Methods)

Hybrid cryptography is another essential concept on the road to quantum-safe security. It refers to the practice of using classical cryptography and post-quantum cryptography together within the same protocol. Instead of replacing RSA or elliptic curve cryptography

immediately, hybrid approaches allow systems to combine both classical and post-quantum algorithms, providing two layers of protection. If one method is ever compromised, the other still ensures confidentiality and integrity.

This principle is important because the transition to post-quantum cryptography will not happen overnight. Many organisations rely on complex infrastructures, legacy systems, long-lifecycle devices, and third-party vendors. These environments cannot be upgraded instantly, and some may take years before they fully support post-quantum algorithms. Hybrid cryptography allows new systems to interoperate with older components safely, ensuring that organisations are protected even during the transition period.

Hybrid approaches also build confidence. Since post-quantum algorithms are new, organisations want an additional layer of assurance while they test and validate their performance. This becomes particularly important in areas like network security, secure communications, cloud platforms, financial systems, and public-key infrastructures. Hybrid cryptography provides this reassurance. It gives organisations the ability to adopt PQC gradually, without taking unnecessary risks or disrupting services.

In practical terms, hybrid cryptography is like fastening both a belt and suspenders before walking into an important meeting. One of them alone might be safe enough, but using both eliminates uncertainty. During the PQC transition, this is the safest approach.

## Principle 3: Algorithm Diversity and Fallback Mechanisms

Another important quantum-safe principle is the idea of algorithm diversity. Cryptography is strongest when it does not rely on a single point of failure. That is exactly why NIST chose more than one algorithm for signatures, selecting both ML-DSA and SLH-DSA. These algorithms are built on different mathematical foundations, which means a weakness in one is unlikely to affect the other. Diversity creates resilience.

In a practical sense, algorithm diversity means designing systems so that if one algorithm becomes insecure, the organisation has a fallback option ready to use. This prevents situations where a single vulnerability compromises critical data. Organisations should consider architectures that allow multiple algorithms to coexist, with the ability to transition smoothly between them when required.

A helpful analogy is having more than one spare key for your car. Even if you misplace the main key, you know you have a backup safely stored at home. That backup prevents panic, saves time, and keeps you mobile. Algorithm diversity serves the same purpose: it prevents cryptographic disruption and ensures continuity of operations in uncertain scenarios.

## Principle 4: Strong Key Management Practices

Quantum-safe cryptography does not eliminate the need for strong key management. In fact, it makes good key management even more important. Post-quantum algorithms often have larger keys and signatures, and they introduce new performance characteristics that organisations must consider. These changes affect everything from network bandwidth to certificate sizes, hardware capabilities, and storage systems.

Quantum-safe key management requires planning for larger certificates, updated hardware security modules, new certificate authority capabilities, and the ability to handle hybrid key exchange methods. At a deeper level, organisations need to avoid hard-coded keys, long-lived credentials, and outdated token formats that may not transition smoothly into the post-quantum era.

The easiest way to visualise this is by imagining that car keys suddenly became much larger. You would need bigger pockets, larger keychains, redesigned ignition slots, and specialised storage boxes. The key still functions, but the environment around it must adapt. Similarly, post-quantum keys work effectively, but they require the supporting systems to evolve with them.

## Principle 5: Zero-Trust and Layered Security Models

Quantum-safe security does not replace the fundamentals of cybersecurity. Instead, it enhances them. The zero-trust model, which operates on the principle of “never trust, always verify,” aligns perfectly with post-quantum thinking. If attackers can harvest encrypted data today and decrypt it in the future, then every communication, transaction, and access point must be verified continuously.

Layered security remains essential as well. Even with quantum-safe algorithms, systems must rely on defence-in-depth strategies that include access controls, authentication, protected identities, monitoring, segmentation, and secure software development practices. Quantum-safe encryption becomes one layer within a broader and more holistic security framework. Relying solely on encryption has never been sufficient, and this becomes even clearer when preparing for advanced computational threats.

## Principle 6: Preparing for an Evolving Cryptographic Landscape

The final quantum-safe principle is recognising that cryptography has entered an era of continuous evolution. Organisations can no longer assume that cryptographic algorithms will remain untouched for decades. Instead, they must treat cryptography as something that requires regular updates, monitoring, testing, and evaluation.

This principle encourages teams to adopt forward-looking practices. It requires staying informed about global PQC standardisation, tracking vendor readiness, participating in industry working groups, and performing periodic cryptographic assessments. It also involves planning for lifecycle management, ensuring that every system can accommodate new cryptographic versions without major disruption.

In many ways, cryptography is beginning to resemble software. It must be maintained, improved, and patched over time. The organisations that successfully embrace this reality will gain a significant advantage in resilience and compliance.

## Conclusion and Strategic Perspective:

As organisations look ahead to the post-quantum world, it becomes clear that cryptography is undergoing one of the most significant transformations in decades. From our perspective, the shift is not only technical but cultural. Organisations that continue treating cryptography as a fixed, invisible component will struggle. In contrast, those that focus on agility, flexibility, and preparedness will navigate this transition with confidence.

The most successful organisations will be those that start early, build awareness, and insist on quantum-safe capabilities from their vendors. They will treat cryptography as something that can change, grow, and adapt. Most importantly, they will understand that becoming quantum-safe is not a single upgrade but a strategic journey.

Quantum-safe principles offer a roadmap for this journey. By embracing crypto agility, hybrid methods, algorithm diversity, strong key management, zero-trust, and continuous evolution, organisations can protect their data for decades to come. And in a world where technology advances rapidly, that kind of long-term resilience is one of the most valuable assets an organisation can build.

---

About the author: Tooba Qasim is a PhD researcher in cybersecurity at City St George's, University of London. Her research includes authentication challenges in Quantum Key Distribution (QKD), analysis of post-quantum cryptography (PQC) algorithms in security protocols and exploring the security and performance of PQC on hardware and resourceconstrained devices.