# Future Innovation and Research

*By Tooba Qasim*

## What Comes After Today's PQC Standards?

It is tempting to think of post-quantum cryptography as a destination. New algorithms are standardised, systems are migrated and the problem is solved.

In reality, post-quantum cryptography is not an endpoint. It is the beginning of a new era of cryptographic change.

The algorithms standardised today represent the *best available answers* to what we know about quantum threats right now. But cryptography has never been static. It evolves in response to new research, new attack techniques, new implementation lessons and new computing paradigms. The quantum-safe future will be no different.

This is why sustainability is not only about maintaining systems but about **anticipating what comes next**.

## PQC Standards Are a Baseline, Not the Finish Line

The current generation of post-quantum cryptographic standards is the result of years of open competition, cryptanalysis and international scrutiny. That process has produced strong, well-reviewed algorithms designed to resist both classical and quantum attacks.

However, history teaches an important lesson: **no cryptographic algorithm lasts forever**.

RSA and elliptic curve cryptography were once considered unbreakable. Over time, advances in mathematics, computing power and attack techniques gradually reduced their safety margins. The same will eventually be true for some post-quantum algorithms, not necessarily because they are "broken," but because better alternatives emerge or weaknesses are discovered at the margins.

This is not a failure of PQC. It is how cryptography works.

Future innovation will include:

- refinements to existing PQC algorithms,
- new parameter sets optimised for different environments,

- entirely new algorithm families,
- and improved implementation techniques that reduce performance and side-channel risks.

Organisations that assume today's standards are permanent will face the same challenges in the future that many face today with legacy cryptography.

## Why Cryptographic Agility Becomes Non-Negotiable

This is where **cryptographic agility** moves from a technical concept to a strategic necessity.

Cryptographic agility is the ability to **replace or upgrade cryptographic algorithms without redesigning entire systems**. In a quantum-safe future, agility is what allows organisations to respond calmly to change rather than scrambling under pressure.

As post-quantum research continues, organisations may need to:

- change algorithms due to new cryptanalytic findings,
- adopt new standards issued by regulators or standards bodies,
- replace early PQC deployments with improved variants,
- respond to vulnerabilities discovered in specific implementations.

Without agility, each of these changes becomes a major engineering project. With agility, they become controlled upgrades.

Future-ready organisations are already designing systems where cryptography is modular, configurable and governed through policy rather than hard-coded into applications and hardware.

## The Role of Research Institutions and Open Science

One of the strengths of the post-quantum transition is how openly it is being developed.

Universities, research institutes, and independent cryptographers continue to analyse PQC algorithms, test their resilience and explore new approaches. This research does not stop once standards are published. In many ways, it accelerates.

Academic work is already exploring:

- tighter security proofs,

- alternative lattice constructions,
- code-based and multivariate cryptography variants,
- improvements in signature size and verification speed,
- implementation hardening against side-channel leakage.

This ongoing research is a feature not a risk. It ensures that weaknesses are discovered early in the open rather than late under adversarial pressure.

Organisations that pay attention to this research ecosystem gain early insight into where cryptography is heading and how standards may evolve.

## AI as an Accelerator of Cryptographic Change

Artificial intelligence will play a growing role in how cryptography evolves.

AI is already being used in cryptographic research to:

- assist in analysing large parameter spaces,
- identify potential weaknesses faster,
- optimise implementations for performance and memory usage,
- automate parts of cryptanalysis and testing.

At the same time, AI changes the threat environment. Attackers can use AI to discover implementation flaws more efficiently, exploit subtle timing or memory behaviours and scale attacks that once required significant manual effort.

This dual role of AI as both a defensive tool and an attack accelerator reinforces the need for agility and continuous reassessment. Algorithms that are secure today may need stronger protections tomorrow, not because quantum computers have arrived but because **AI has changed how attacks are executed**.

## Beyond Algorithms: New Cryptographic Building Blocks

Future innovation will not focus solely on encryption and signatures.

Research is increasingly looking at:

- privacy-preserving computation,

- secure multi-party protocols,
- post-quantum authentication methods,
- cryptographic mechanisms for distributed and decentralised systems,
- integration with zero-trust and identity-centric architectures.

Post-quantum cryptography will become one layer in a broader security stack rather than a standalone solution. Organisations that view PQC as a narrow technical upgrade risk missing these wider shifts.

## Why This Matters for Long-Term Strategy

The key insight for sustainability is simple: **quantum-safe security is a moving target**.

Future-ready organisations are not asking only "Which PQC algorithms should we deploy?" They are asking:

- How easily can we change them?
- How do we track emerging research?
- How do we adapt without disruption?
- How do we align cryptographic evolution with cloud, AI and zero-trust strategies?

The answers to these questions define whether an organisation remains secure over decades rather than just passing a compliance milestone.

## Looking Ahead

The post-quantum era will be shaped as much by research and innovation as by standards and regulation. New ideas will emerge, assumptions will be challenged and best practices will evolve.

Sustainability is about embracing that uncertainty not resisting it.

Organisations that build cryptographic agility, stay connected to research communities and treat PQC as part of a living security strategy will be the ones best prepared for whatever comes next.

The future of quantum-safe security will not belong to those who pick the "right" algorithm once. It will belong to those who can **adapt repeatedly, confidently and deliberately**.