QUANTUM
THINK TANK

Insight that protects. Foresight that leads

# Post-Quantum Cryptography Fundamentals

By Tooba Qasim

January 2026

www.cyberlondon.com | info@cyberlondon.com

## A Simple Introduction to Post-Quantum Cryptography

If you have been hearing the term post-quantum cryptography (PQC) and wondering what it means, you are not alone. Quantum computing sounds like something from a sci-fi movie and adding cryptography on top can feel even more confusing. But don't worry. In this article, we will break things down in plain language, using simple examples so that anyone technical or not can understand what is going on and why organisations need to care.

## What Is Post-Quantum Cryptography?

Let's start with the basics.

Today, almost everything we do online sending emails, using a banking app, logging into a website is protected by encryption. Encryption is like a digital lock that only the right key can open.

But here is the catch: those locks were designed for *classical computers*. Quantum computers work very differently, and once they become powerful enough, some of our most important digital locks could suddenly become breakable.

Post-quantum cryptography (PQC) is the next generation of digital locks designed to stay secure even in a future where quantum computers exist and are powerful enough to cause harm. Think of it like upgrading from a regular padlock to a high-security lock that even a futuristic laser cutter can't break.

## Why Do Today's Encryption Methods Become Weak in the Quantum Era?

Right now, the two main types of encryption we rely on are:

- **RSA (Rivest-Shamir-Adleman)**
- **ECC (Elliptic Curve Cryptography)**

These systems are secure today because breaking them would require a classical computer to try trillions of guesses, something that would take thousands or even millions of years.

But quantum computers use quantum physics to perform computations in parallel. A strong quantum computer could use an algorithm called **Shor's algorithm** to break RSA and ECC **in hours or minutes**, not centuries.

This creates a problem known as:

**"Harvest Now, Decrypt Later"**

Attackers can **collect encrypted data today** and simply **wait** until they eventually have a quantum computer capable of unlocking it.

This is especially dangerous for:

- Sensitive personal information
- Government communications
- Financial data
- Long-term intellectual property
- Medical and genomic data

If that information is supposed to stay private for 10, 20, or 50 years, then it is already at risk.

## What NIST Has Done: The Standardisation Process

The good news?
We are not starting from scratch.

The U.S. National Institute of Standards and Technology (NIST) has spent **years** running a global competition to identify mathematical systems that could replace RSA and ECC in a quantum-safe world. After examining dozens of candidate algorithms from researchers worldwide, and after extensive testing, NIST selected **three algorithms** for standardisation.

These are now considered the global starting point for quantum-safe cryptography.

## Meet the New PQC Algorithms

Let's look at the three approved algorithms using simple, real-life examples. No equations. No math headaches. Just concepts.

Their older research names (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+) are still widely recognised, but they now have formal standard names:

- **ML-KEM** (formerly CRYSTALS-Kyber)
- **ML-DSA** (formerly CRYSTALS-Dilithium)
- **SLH-DSA** (based on SPHINCS+)

### ML-KEM (formerly CRYSTALS-Kyber) - Encryption / Key Establishment

Think of ML-KEM like a super-secure locker in a train station.

Imagine you want to share something valuable with someone far away. You both agree to use a locker in a station that only you two can access.

Today's encryption works by leaving the locker number and key inside a puzzle box. A classical computer needs thousands of years to solve that puzzle box, so it's safe.

**But a quantum computer?**
It would open the puzzle box instantly.

ML-KEM solves this by working differently:

- Instead of a puzzle box, its lock changes shape every time someone looks at it.
- Even if attackers are watching closely, they can't figure out how the lock works.
- Only you and the intended person can open the locker.

**In simple terms:**
ML-KEM helps two people create a shared secret key safely even if attackers with powerful quantum tools are listening in.

For full technical details, see the official FIPS specification document here.

### ML-DSA (formerly CRYSTALS-Dilithium) - Digital Signatures

Think of ML-DSA like your **hand-drawn signature but impossible to forge**.

When you sign a paper document, your signature proves that you approved it. But signatures can be forged.

Digital signatures try to fix that, they are like a digital stamp that only your computer can make.

The issue?
Quantum computers could eventually forge today's digital stamps.

ML-DSA fixes that by creating signatures that are:

- **Easy for you to generate**
- **Easy for others to verify**
- **Extremely hard even for quantum computers to fake**

A simple way to picture it:

It is as if your signature were made of thousands of tiny dots arranged in a pattern only you can create.

If someone tries to copy it, even slightly, it instantly looks wrong.

**In simple terms:**
ML-DSA proves that a message, transaction, or software update really came from you and it can't be forged by quantum attackers.

For full technical details, see the official FIPS specification document here.

### SLH-DSA (based on SPHINCS+) - Backup Signature Scheme

Think of SLH-DSA like sealing a document inside many, many envelopes.

You write a message and seal it inside an envelope.
Then you put that envelope in a second one.
Then a third.
And you keep going, hundreds or thousands of layers deep.

To reach the message, you would need to know exactly which envelope to open at each step.

That is essentially how SLH-DSA works:

- It uses layers of hashing, a very secure, one-way process.
- Even quantum computers can't easily reverse these layers.

- It is extremely conservative and heavily tested, which is why it is considered a “safety net”.

It is slower and larger than ML-DSA, so it is not the main signature algorithm but it is ideal as a backup.

In simple terms:
SLH-DSA is your “**belt and suspenders**” approach to signatures.
It is slower but incredibly reliable, your backup parachute in case anything goes wrong with the main algorithm.

For full technical details, see the official FIPS specification document here.

**What Is “Hybrid Cryptography” and Why Do We Need It?**

You might assume we can simply replace RSA and ECC with the new algorithms and call it a day.
But things in the real world are rarely that simple. Most organisations will use **hybrid cryptography** during the transition phase.

This means:

**Combine classical encryption (RSA/ECC) with post-quantum algorithms at the same time.**

It is like wearing both a belt and suspenders until you are completely sure the new system works.

Hybrid encryption gives organisations:

- backward compatibility
- extra reassurance while PQC is rolled out
- protection against early bugs or unexpected issues
- time for systems and vendors to catch up

Eventually, we will move fully to PQC but hybrid modes help bridge the gap safely.

## Why PQC Is Not “Plug-and-Play”

If moving to Post-Quantum Cryptography were as simple as installing an update or pressing a button, organisations would have already done it.

In reality, PQC affects almost every part of a digital environment, and that makes the transition far more complex than it appears. Here is why it is more complicated:

### 1. Encryption is everywhere, even in places people don't realise

Modern IT systems rely on encryption in thousands of hidden layers.
It is not just used in obvious places like secure websites or VPNs, it sits deep inside:

- servers and databases
- cloud platforms
- identity and authentication tools
- email systems
- mobile apps
- payment systems
- IoT devices and sensors
- backup systems
- internal APIs
- network protocols (TLS, SSH, IPSec)

Many organisations don't even have a complete list of where cryptography lives.
Before PQC can be introduced, you must identify all encryption points.
This "crypto inventory" alone can take months in large organisations.

### 2. PQC has larger keys, signatures, and computational requirements

PQC algorithms are secure against quantum attacks, but this comes at a cost:

- keys are larger
- signatures are larger
- ciphertext sizes may increase
- operations may require more memory

Some older systems struggle with these larger sizes.
For example:

- legacy applications may break because they expect small RSA keys

- embedded systems may not have enough memory for PQC
- network performance can slow down without optimisation

PQC migration therefore requires testing, tuning and sometimes redesigning systems, not just swapping algorithms.

3. **Hardware may need upgrades**

Many devices have cryptography built into firmware or chips. Examples:

- smart cards
- ATMs
- industrial control systems
- routers and switches
- IoT sensors
- hardware security modules (HSMs)

These devices often cannot support PQC unless:

- firmware is updated, or
- the physical hardware is replaced.

This makes PQC adoption slower, especially in sectors with large amounts of legacy equipment (healthcare, manufacturing, transportation).

4. **Vendors are not aligned, everyone is moving at a different speed**

Your environment is a mixture of:

- cloud platforms
- security vendors
- hardware manufacturers
- software providers
- open-source libraries

Some vendors already support PQC testing. Others are experimenting. Others have not started.

This means you cannot fully move to PQC until your supply chain is ready. Organisations must coordinate with vendors, request roadmaps, and prepare hybrid solutions in the interim.

**5. Compliance, standards and audit requirements are still evolving**

Regulators and industry bodies are still writing guidance for PQC. Examples:

- NIST finalising standards
- NCSC issuing best practices
- ETSI developing technical specifications
- US and EU drafting migration guidance
- Audit frameworks slowly updating to include quantum-safe expectations

Because nothing is fully finalised yet, organisations must:

- design flexible solutions
- avoid locking themselves into one design
- prepare for updates over the next few years

This is why crypto agility is essential, systems must be able to switch algorithms again in the future.

**Final Thoughts: Start with Understanding**

The shift to post-quantum cryptography is not about science fiction it is about future-proofing.
Quantum computers aren't breaking encryption today, but the data you are protecting today may still matter many years from now.

PQC is the foundation of the next generation of cybersecurity. And like any major change, the first step is simply **understanding what is coming and why it matters**.

---

*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*