



**DR SHARLENE
THIAGARAJAH**
TM Research &
Development CEO

EVERY time we bank online, access a cloud service or send sensitive information, cryptography is working quietly in the background.

Most of us never see it. We simply expect our information to stay private and our digital transactions to remain secure.

For organisations, however, that invisibility creates a challenge.

As we prepare for a future where quantum computing could affect some of today's encryption methods, the question is no longer only whether organisations should prepare.

The more practical question is: do they actually know where cryptography is being used across their systems today?

This matters because Malaysia is already moving towards greater quantum readiness.

The National Cyber Security Agency's (NACSA) MyKriptografi Action Plan 2026-2030 translates the National Cryptography Policy into coordinated programmes to strengthen Malaysia's cryptography ecosystem, accelerate the use of trusted cryptographic technologies and prepare for emerging cybersecurity challenges, including the quantum computing era.

So where should organisations begin?

Start by knowing what you have

Cryptographic technologies are used to authenticate the source of information and protect the confidentiality and integrity of information we communicate and store.

In simple terms, cryptography uses mathematical functions, often with keys, to protect data. But in a large organisation, cryptography can be everywhere.

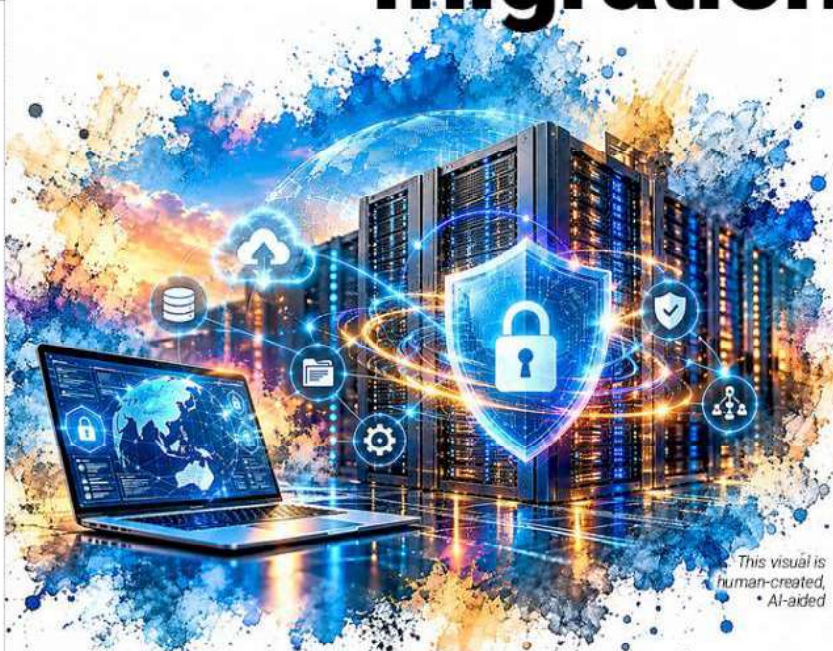
In practice, public-key cryptography is integrated into computer and communications hardware, operating systems, applications, communications protocols, key infrastructures and access-control mechanisms.

That means it can be spread across many parts of an organisation's technology environment.

The US National Institute of Standards and Technology (NIST), through its National Cybersecurity Centre of Excellence (NCCoE), says a good place to start post-quantum migration is to perform cryptographic asset discovery and inventory across an organisation's systems.

A cryptographic inventory is a descriptive record of the cryptography used across systems, appli-

Setting up quantum-safe migration



This visual is human-created, AI-aided

■ Cryptography is spread across many parts of an organisation's technology environment

■ Migration needs to be planned rather than treated as a single technology change

■ A quantum-safe future begins with knowing what you have and understanding what matters

cations, services; devices and data flows.

Think of it as a map of an organisation's digital security environment – what cryptography is being used, where it is used and what it protects.

NIST notes that maintaining a cryptographic inventory is an important step in quantum readiness because organisations cannot effectively prioritise or migrate cryptography they have not identified.

It is a little like renovating an old building. Before replacing the wiring, you need to know where it runs, what it connects to and what could be affected when you start changing it.

Not everything needs to move at once

Once organisations know what they have, the next challenge is deciding what matters most.

A cryptographic inventory may also include information about the data being protected, especially sensitive or long-lived data.

Once organisations know where cryptography is used, they can begin to decide which systems need attention first.

Malaysia's NACSA guidance takes a similar risk-based approach, calling for a risk register and dependency assessment to identify migration risks, system criticality and the impact of legacy cryptography and dependencies.

This is important because migration needs to be planned and prioritised rather than treated as a single technology change.

NIST says post-quantum cryptography (PQC) migration

requires organisations to understand where quantum-vulnerable public-key algorithms are used across hardware, software and services, and to develop roadmaps that prioritise the use of NIST's PQC algorithms.

The aim should not be to replace everything overnight.

It should be to understand where the greatest exposure lies and move in a structured way.

From discovery to action

An inventory is useful only if it leads to action.

NACSA sets out five national migration phases: Assess. Select. Validate. Deploy. Monitor.

The phases are intended to help organisations plan resources more systematically and carry out migration activities according to priority.

In practical terms: understand what you have, decide what needs to change, test it, implement it and keep monitoring it.

This is where the conversation moves beyond simply keeping a list of cryptographic assets towards managing an organisation's wider cryptographic posture. This moves quantum-safe migration beyond a one-off technology replacement.

The larger goal is to build an environment where organisations understand their cryptographic dependencies and can respond more easily when change is required.

Build for the next change too

This is where crypto-agility becomes important.

In my previous article, I described it using a simple analogy: instead of rebuilding the entire house whenever security improves, we should be able to change the locks.

NIST describes crypto-agility as the capability to replace or adapt cryptographic algorithms across protocols, applications, software, hardware, firmware and infrastructure, while maintaining security and ongoing operations.

Put simply, it asks a practical question: can you change your cryptography when you need to, without breaking your business?

It also notes that the transition to PQC has highlighted significant challenges in adapting applications to new algorithms.

The objective, therefore, should not simply be to move from today's algorithm to tomorrow's algorithm, but to make the next change easier too.

Malaysia has a good reason to keep moving. It is the only Asean country to reach Tier 1 in the Asean Post-Quantum Cryptography Readiness 2026 assessment.

According to the National Security Council, the assessment was based on verifiable national-level actions and implementation rather than stated intentions alone.

Malaysia's preparations include cryptographic asset inventories, risk assessments, capability development, technology testing and phased migration. The next step is to keep translating that national readiness into practical capability within organisations.

At TM R&D, we are building capability with Multimedia University in cryptographic discovery using an agentless approach, working closely with Prof Ts Dr Heng Swee Huay, member of the Centre of Intelligent Cloud Computing under CoE for Advanced Cloud.

The plan is to strengthen competencies in cloud security and cryptography, particularly PQC and digital signature.

We are also collaborating with partners to strengthen end-to-end cryptographic posture management.

The focus is practical: improving visibility of cryptographic assets and building the foundations needed for assessment, remediation and future migration.

Preparing for a quantum-safe future does not begin with replacing everything.

It begins with knowing what you have, understanding what matters most and being ready to adapt.

In a quantum-safe future, readiness starts not with replacing everything, but with knowing where to begin.