eBook

Post-Quantum Cryptography

Preparing your organization for a quantum future today

cpl.thalesgroup.com

THALES
Building a future we can all trust

A brief history of quantum

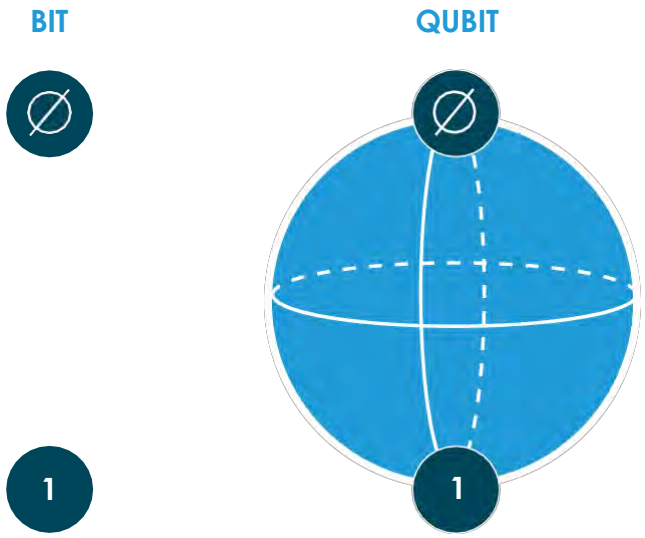
QUANTUM COMPUTERS ARE NOT SCIENCE FICTION

Rather than being reserved for science fiction movies, quantum computers exist today as organizations drive towards commercialization.

- Google's Sycamore computer boasts 70 qubits (quantum bits)-Aug 2023.
- IBM's Osprey quantum processor with 433 qbits is the most powerful in the world, and the company plans to hit the 4,000-qubit stage with its Kookaburra processor in 2025.
- Tech firms including Google, IBM, Microsoft, and Amazon have announced quantum computing available in the cloud as a service.

QUBITS: THE BUILDING BLOCKS OF A QUANTUM COMPUTER

- Classical bit: 0 or 1
  Qubit: Superposition of 1 and 0
- 'N' Entangled qubits represent all 2N states simultaneously
- When measured, all states collapse but one
- Objective is to make the measured state represent something useful



OBSERVING THE 20-YEAR MARK OF QUANTUM COMPUTING GROWTH

Quantum computing systems produced by organization(s) in qubits, 1998 - 2019.

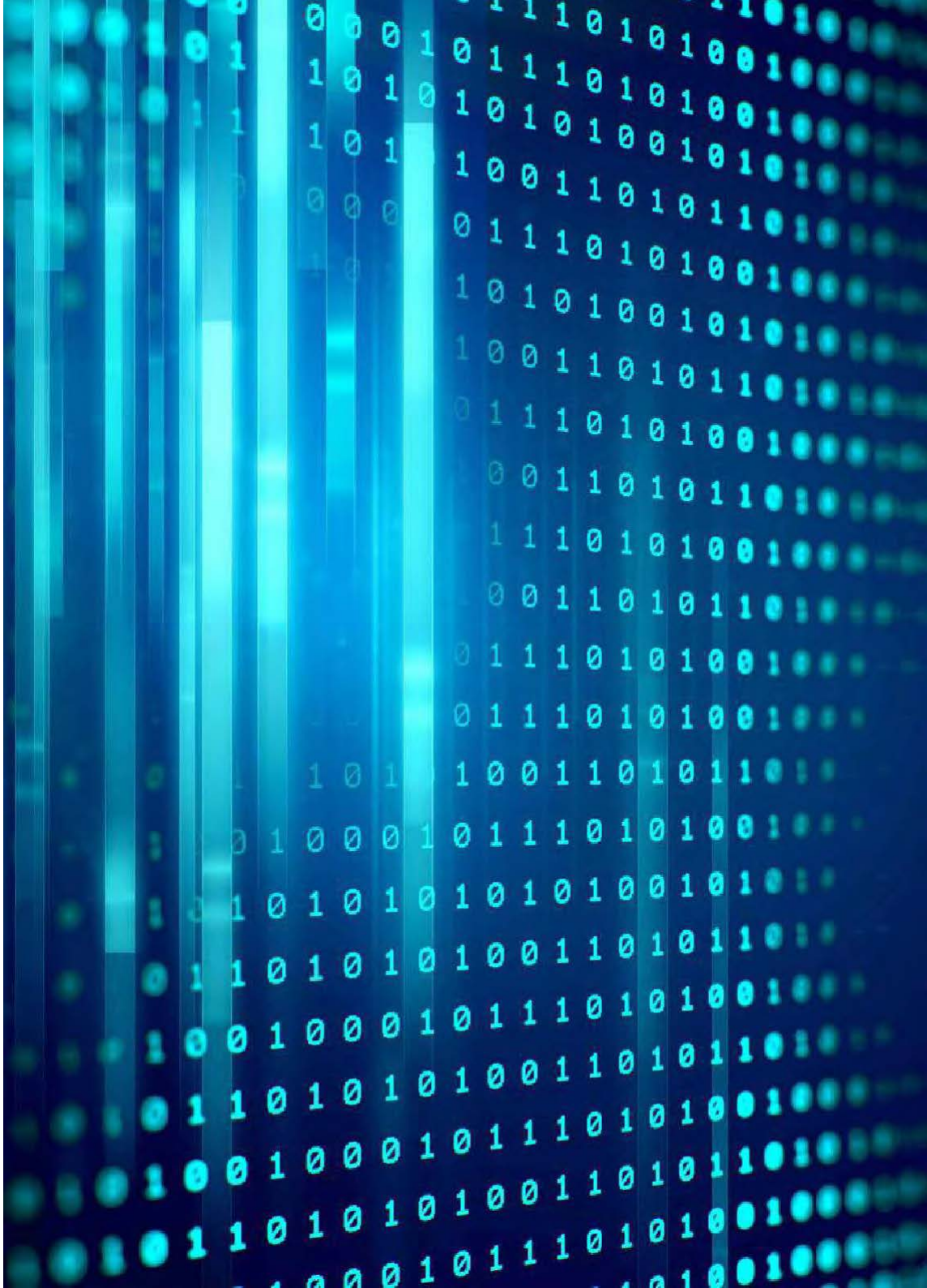
Source: CB Insights

WHEN WILL QUANTUM COMPUTING AFFECT ORGANIZATIONS?

73% Recognize the future threat of quantum computing

39% Have defined a quantum-related security strategy

Security Weaknesses in Data in Motion Identified in Cybersecurity Survey
Global research report of IT and cybersecurity decision makers-TechTarget and Thales



HOW REAL IS THE THREAT?

TIMEFRAME (TO DEVELOP LARGE SCALE PQC)	IMPACT	LIKELIHOOD	RISK
Short term (1-5 years)	HIGH	LOW	MEDIUM
Medium term (5-10 years)	HIGH	MEDIUM	HIGH
Long term (10-20 years)	HIGH	HIGH	EXTREME

There is NO low risk outcome

Quantum-safe security

Post-Quantum Cryptography

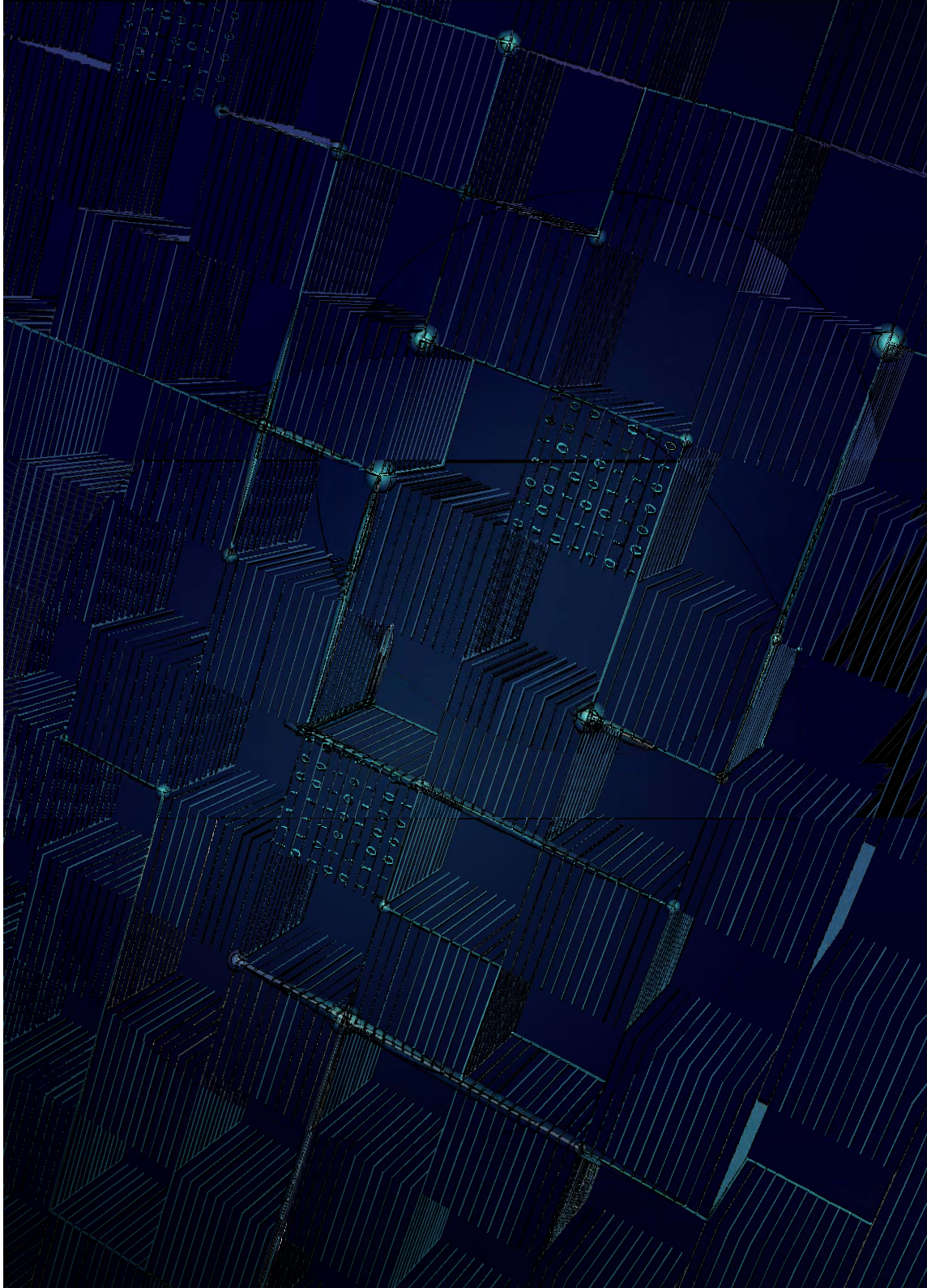
The introduction of post-quantum cryptography (PQC) will provide long-term protection for government and commercial data against the emerging threat of quantum computing. Quantum computers will render today's conventional public key encrypted infrastructures unsecure.

Using a hybrid encryption model, PQC enables customers to combine both classical and quantum-resistant algorithms in a single platform, providing a secure transition to a post-quantum world.

PQC is available to all current and future customers as part of Thales' crypto-agile platform. At Thales, we recognize organizations must adopt a strong post-quantum crypto-agile strategy. In preparation for the transition, Thales encourages organizations to practice crypto-agility now, to help your organization evolve and avoid expensive security retrofitting in the future as quantum computing becomes more established.

This design principle facilitates changes to the cryptography even after deployment and allows you to prepare for the transition to quantum-safe solutions once the NIST standardization process is completed.

To this end, Thales already offers crypto-agile HSMs, key management, and network encryption solutions that you can take advantage of today.



“Without quantum-resistant encryption, everything that has been transmitted, or will ever be transmitted over a network, will be vulnerable to eavesdropping and public disclosure.”

ETSI White Paper No. 8 Quantum Safe Cryptography and Security

THE IMPORTANCE OF CRYPTO-AGILITY & QUANTUM-READINESS

The world depends on Public Key Infrastructure (PKI) to establish trust.

PKI depends on asymmetric key protocols such as RSA, ECC and others.

Quantum computers and research will efficiently crack PKI and code signing.

Post-quantum cryptography (PQC) will ensure that sensitive data remains encrypted into the future.

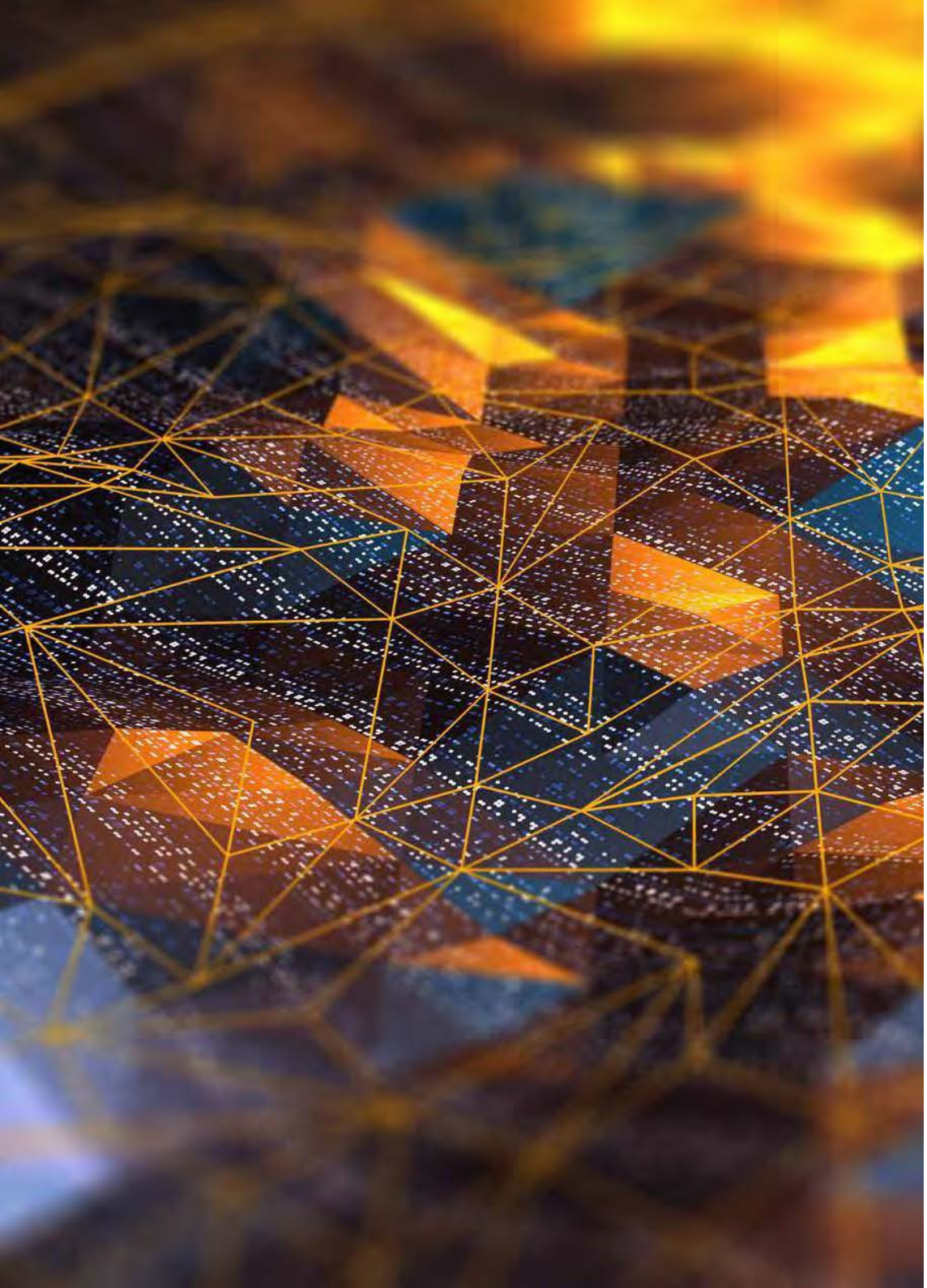
WHO IS COMING TO THE RESCUE?

In 2022, NIST selected four algorithms designed to withstand attack by quantum computers. In 2023, standards for three of the four were released, with standards for **FALCON** to come in 2024:

- **CRYSTALS-Kyber ML-KEM**
- **CRYSTALS-Dilithium ML-DSA**
- **SPHINCS+ SLH-DSA**
- **FALCON**

“The best way to start preparing is to ensure that all current and future systems have cryptographic agility – the ability to be easily reconfigured to add quantum-resistant algorithms.”

Dr. Brian LaMacchia,
Distinguished Engineer and Head of the Security and Cryptography Group at Microsoft Research



QUANTUM DEFENSES #1: QUANTUM-RESISTANT ALGORITHMS

Designed specifically to resist against quantum attack, quantum resistant algorithms (QRAs) are being designed using a range of methods:

- Lattice-based cryptography
- Multivariate cryptography
- Hash-based cryptography
- Code-based cryptography

Performance in real-world protocols varies (key sizes, padding schemes, latency) and the standards are evolving at present.

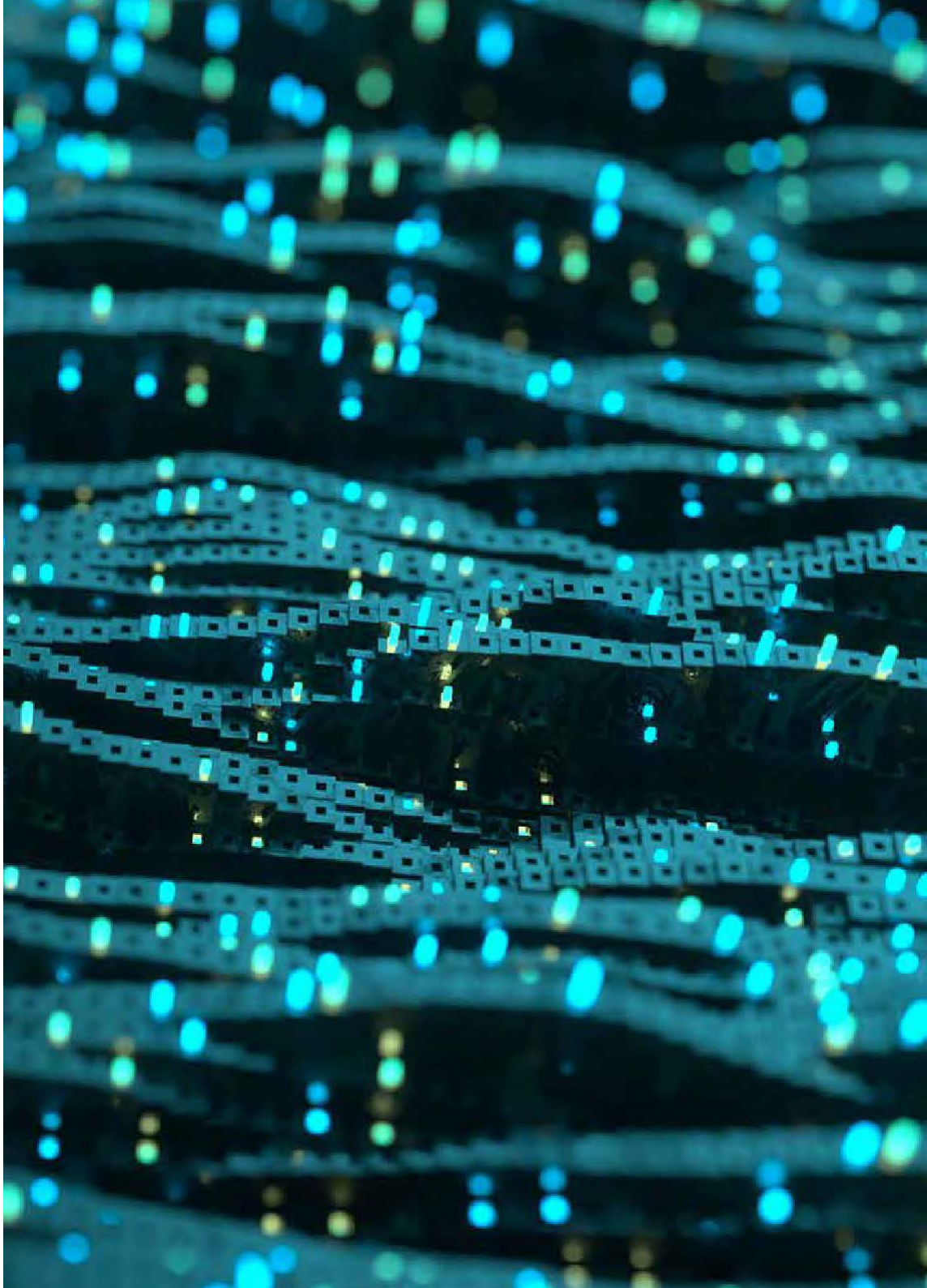
These will look at digital signatures, public key encryption and key encapsulation mechanisms.

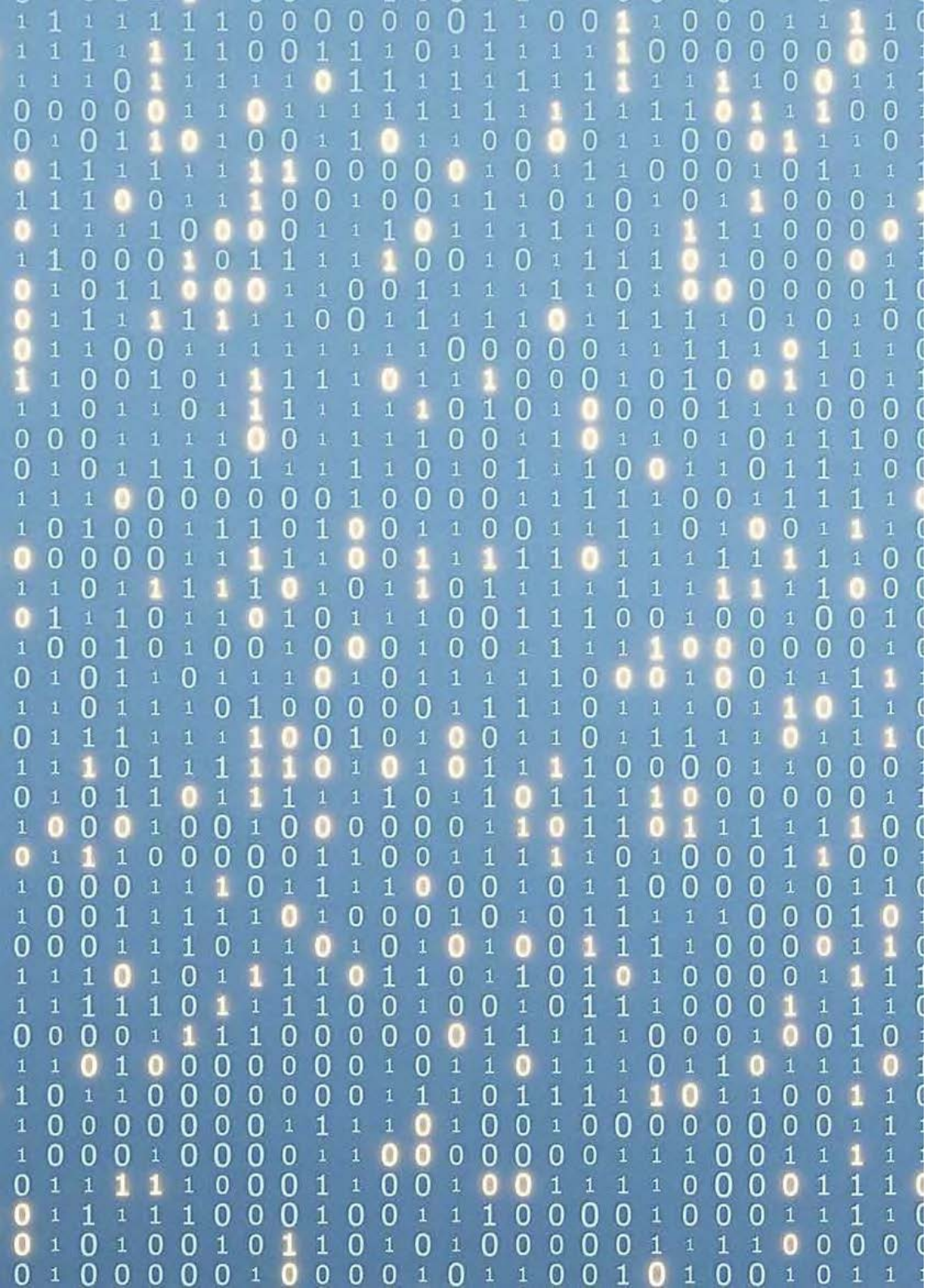
QUANTUM DEFENSES #2: QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD) can be used to:

- Aid forward secrecy by harnessing properties of quantum mechanics
- Provide a fundamentally different approach to key sharing
- Distribute keys based on principles of physics, not mathematics

QKD can be deployed across telecoms' networks, mitigating the risks of data breaches.





QUANTUM DEFENSES #3: QUANTUM ENTROPY

Quantum Random Number Generation (QRNG) can be used to:

- Provide a high bit rate random number source
- Harness inherent randomness in quantum mechanics
- Seed truly random encryption keys
- Secure a range of devices and applications, from IoT to online gaming

A HYBRID APPROACH TO DATA ENCRYPTION

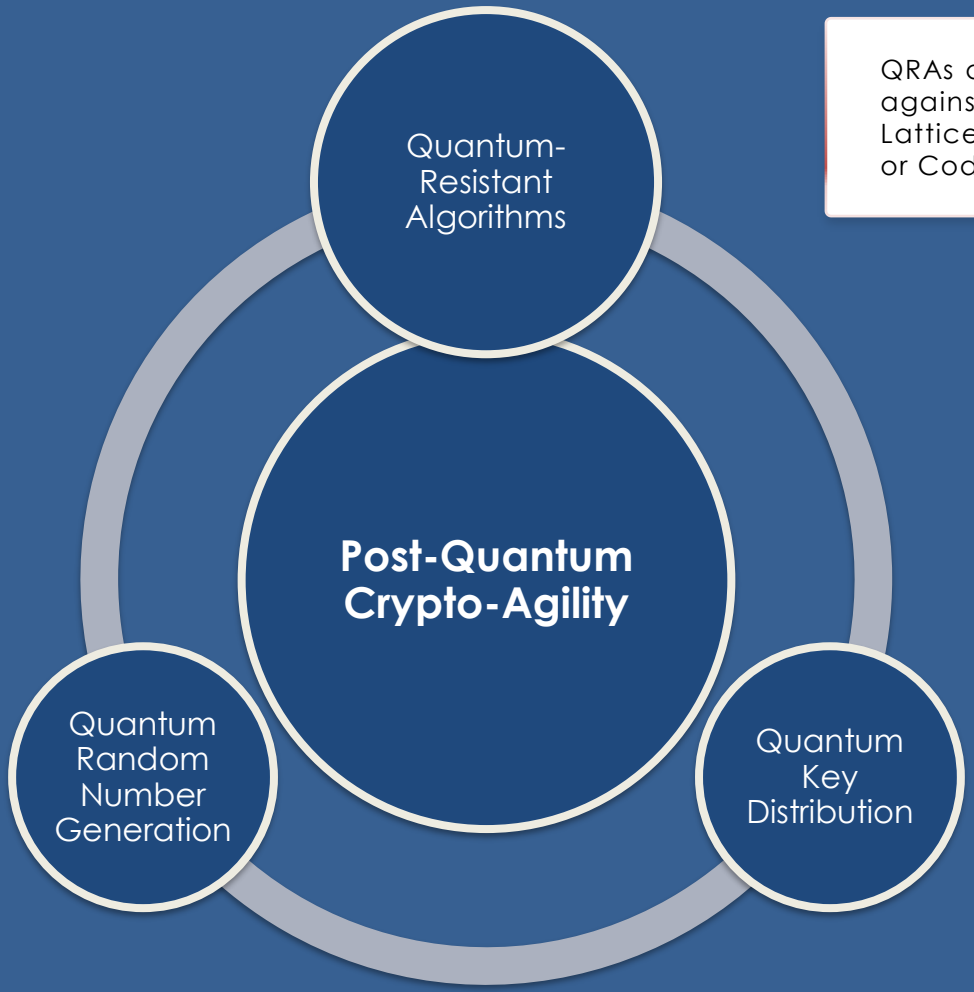
NIST recommends a hybrid approach to cryptography, utilizing crypto-agile platforms for a smooth transition.

In practice this means:

- Algorithms – Support for alternate modes with classical algorithms and QRA
- QKD - Leverage quantum mechanics for key establishment and distribution
- RNGs – Combine QRNGs with NIST certified RNGs

Hybrid encryption refers to the use of both proven classical encryption algorithms AND quantum-resistant encryption algorithms. Hybrid encryption requires a crypto-agile platform and ensures long-term data protection in a post-quantum world.

BUILDING A FUTURE-PROOF QUANTUM STRATEGY



QRAs are fundamental to protecting against quantum attacks, whether using Lattice based, Multivariate, Hash based, or Code-based cryptography

QRNG is a high bit rate random number source harnessing the inherent randomness in quantum mechanics to create encryption keys

QKD distributes encryption keys between shared parties based on the principles of quantum physics and the properties of quantum mechanics

RISK FOCUS AREAS

With past and future transactions at risk, its crucial to focus on these critical areas:

Key Management

- Key management
  - Keys vulnerable to loss, theft or corruption
  - Operating system & application vulnerabilities put keys at risk
  - Subject to virtual & cloud cloning attacks
- Keys & data stored together
  - If you can access the encrypted data, you can access the key
- No assurance of keys
  - Varied access methods create security & access issues

Data in motion

- Long-term data often moved between data centers
  - 100 Gbps (or more) at risk!
- Data in motion is often harvested
  - Siphoned from lines and held for future use
- By the time you know, it's too late!
  - Data-in motion breaches are under reported

KEY TAKEAWAYS

Quantum is coming

Quantum capabilities are accelerating

NIST and others are finalizing quantum-safe standards

PKI-based crypto will become obsolete

Know your risks

Long -term data is at risk, if using classic technologies

Consider that it is vulnerable to harvesting and early attacks

Focus on crypto agility

Crypto-agility is the best practice; requires supporting infrastructure

Take a hybrid approach by using classic & quantum-safe crypto solutions

Start now

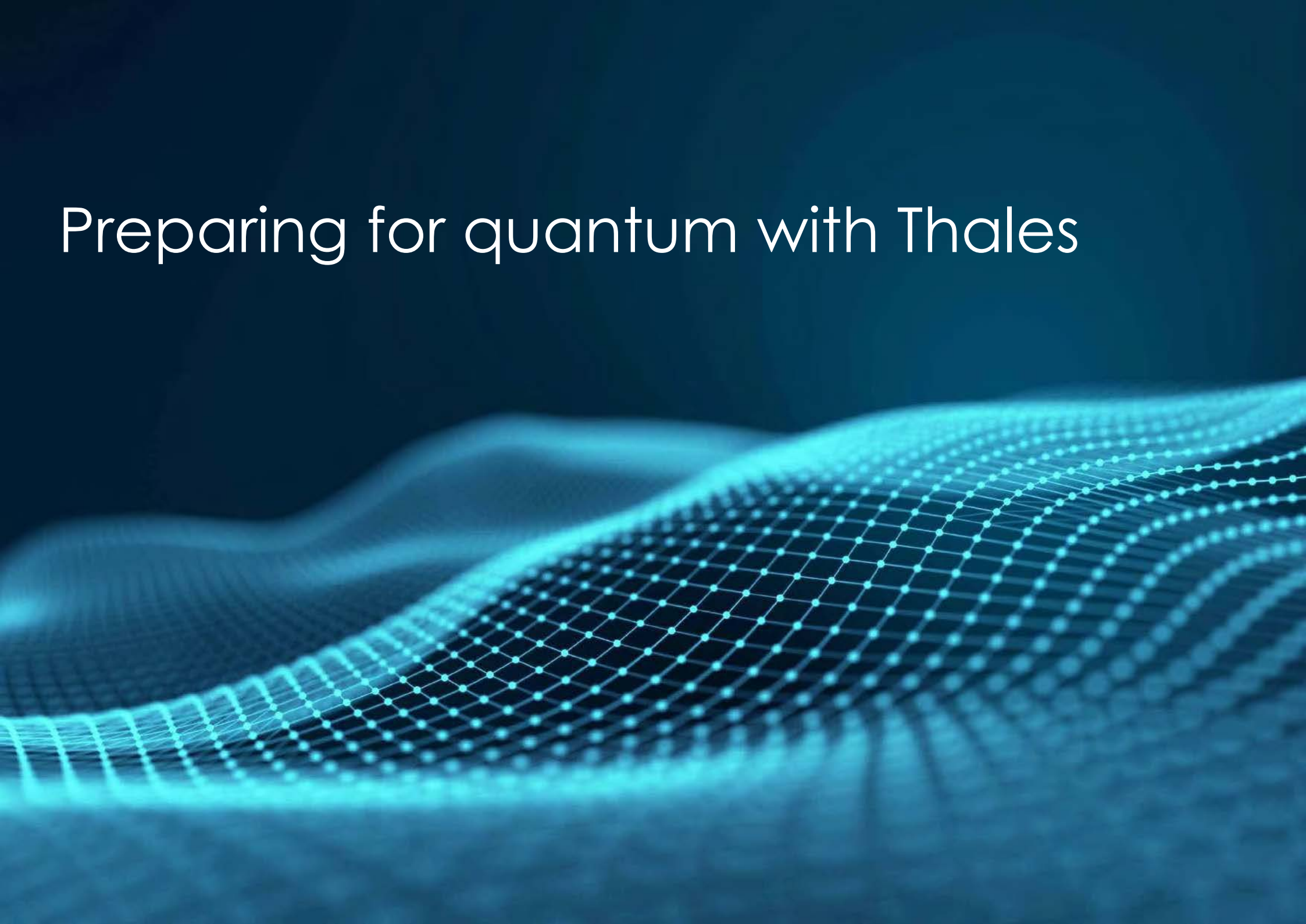
Assess your crypto-agility maturity and readiness

Design a quantum-safe architecture

Be ready for change, even after standards are established

Thales has solutions and partnerships in place today to support your quantum-safe initiatives

Preparing for quantum with Thales



PREPARING FOR QUANTUM TODAY WITH THALES

PRACTICE

Crypto-Agility

Thales Luna Hardware Security Modules (HSM)

APPLY

Quantum Key Generation

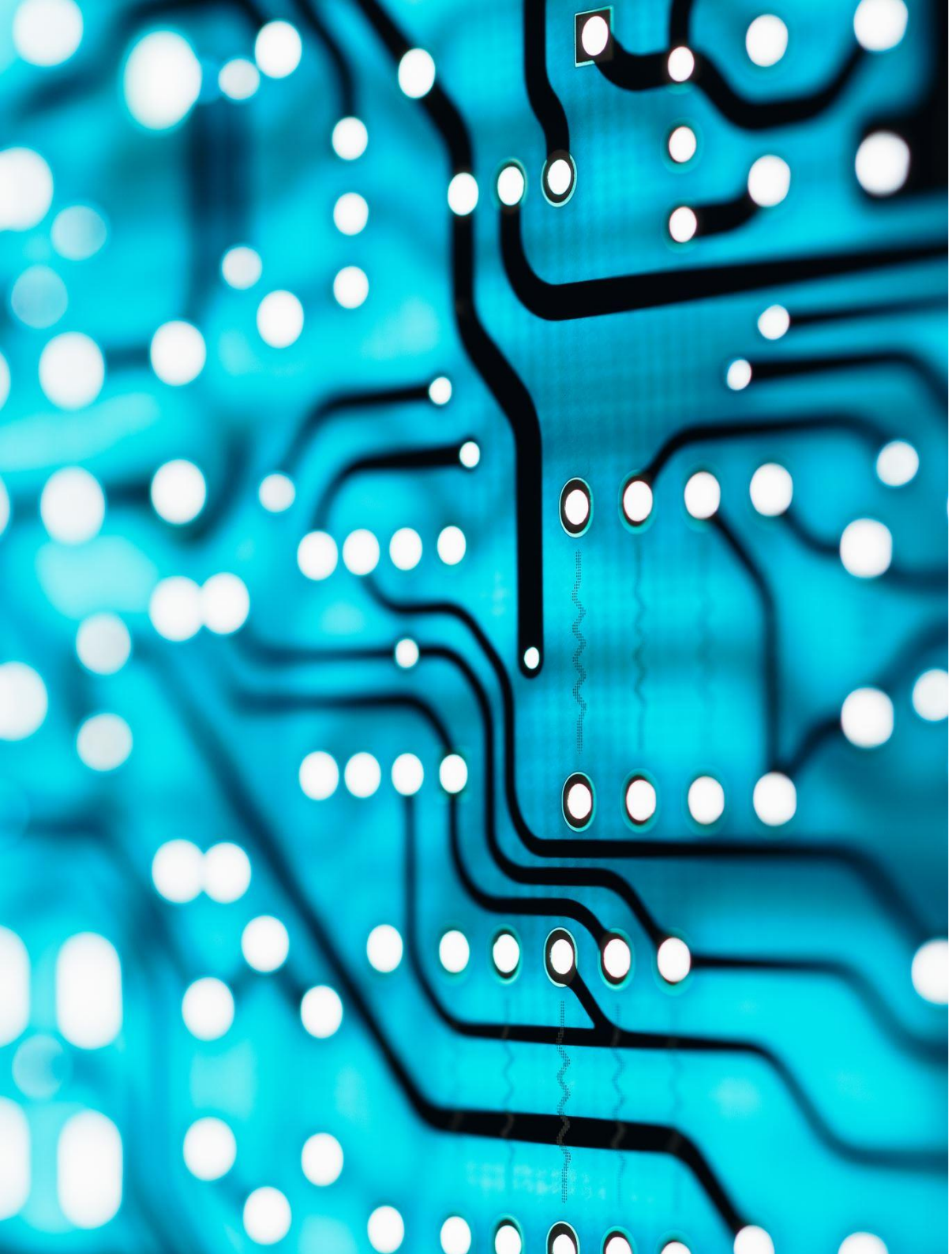
IMPLEMENT

Quantum-Resistant Algorithms

Thales High Speed Encryptors (HSE)

LEVERAGE

Quantum Key Distribution



LUNA HSM APPROACH TO QUANTUM

Luna HSMs provide a crypto-agile approach to ensure PQC-readiness:

- Work with our technology partners
- Work with standard bodies
- Focus on code signing
- Add NIST quantum resistant finalists

COMMERCIALLY AVAILABLE QUANTUM-SAFE LUNA HSMs

Quantum-Resistant Algorithms with PQC FM

HSM protects quantum-safe keys:

•Hash Based Signing (SP 800-208)
- HSS – Hierarchical Signature Scheme (multi-tree version of LMS)
- XMSS – Extended Merkle Signature Scheme
- XMSSMT – XMSS Multi-Tree

•SPHINCS+ (SLH-DSA)
•Kyber (ML-KEM)
•Dilithium (ML-DSA)

Integrated /Custom-made PQC

Implement your own Post-Quantum Crypto using Luna's Functionality Module (FM)

Use various Partner FMs/integrations

QRNG

Inject quantum entropy with QRNG and Luna HSM's secure key storage

Address critical applications where high-quality random numbers are vital

HSE QUANTUM-READY USE CASES

High Speed Encryption can help secure many environments including:

- Data Center Interconnect
- Financial Services
- Government
- Critical National Infrastructure

Thales HSE QUANTUM DEFENSES

CRYPTO-AGILITY

Thales' crypto-agile and high-assurance encryption solutions offers:

- The ability to quickly modify underlying crypto primitives
- Flexible upgradeable technology
- No built-in obsolescence

This ensures organizations can quickly adapt in an ever-evolving cybersecurity landscape.

- Full separation of crypto-security duties
- Compatible with external sources of entropy
- Field-programmable FPGA encryption engine
- Quantum-ready (compatible with QKD)
- Supports CFB, CTR and GCM encryption modes
- Self-healing key management
- Support for AES 128- & 256-bit algorithms

Commercially available Quantum-safe High Speed Encryptors

Quantum Resistant Algorithms

Framework to support QRA

OQS

Quantum Key Distribution

HSE has supported QKD for over a decade

QRNG

QRNG is integrated into the HSE solution

ETSI

IDQ

QUANTINUUM

Crypto-Agility

HSE supports Post Quantum Cryptography (PQC) with a crypto-agile, FPGA-based architecture

Thales Cloud Protection & Licensing

Our Solutions

- Data Security
- Access Management & Authentication
- Software Monetization

Over 2,600 employees

25 countries presence

750 engineers worldwide

30,000 customers worldwide

Thales's technologies and services help secure more than 80% of all global payment transactions and increasingly valuable corporate and government information

The people we rely on to secure our privacy rely on Thales

#1 Worldwide in general-purpose HSMs	#1 Worldwide in data encryption
#1 Worldwide in payment HSMs	#1 Worldwide in key management
#1 Worldwide in cloud HSMs	#2 Worldwide in cloud authentication
#1 Worldwide in software protection	#1 Worldwide in software licensing

THALES

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data.

When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

Contact Us

For all office locations and contact information, please visit

cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com