# < THE QUANTUM THREAT & POST-QUANTUM  CRYPTOGRAPHY >

UNDERSTANDING THIS MAJOR SECURITY ISSUE
AND WHY WE NEED TO ACT NOW

POST-QUANTUM CRYPTOGRAPHY WORKGROUP

CAMPUS CYBER

# EDITO

*One of the commitments of Campus Cyber is to get French and European players working hand in hand, with the aim of disseminating our Members' knowledge while helping to improve the general cybersecurity of our institutions.*

*This document, co-produced by the PQC working group of our «Studio des Communs», has been reviewed, commented on, and expanded by experts in post-quantum cryptography from the Netherlands, including our friends Ms Anita Wehmann, Mr Germain van der Velden, Professor Ronald Camer, and their teams. This work bears witness to the importance of collaboration, a fortiori European collaboration, on such complex subjects. Campus Cyber is proud to support these initiatives, and this major work, co-led by our valued Members and Partners.*

*Anticipation and collaboration are two major objectives that will enable us to build a «cyber-serene» future together. Post-quantum cryptography - securing our sensitive data using algorithms that will resist quantum computers - is a subject for the years to come that must be tackled now. Security managers, business leaders, and politicians need to be made aware of the importance of maturity on these issues. Attacks already exist, as do official recommendations, in particular those put forward by the ANSSI in their advisories published over the last two years.*

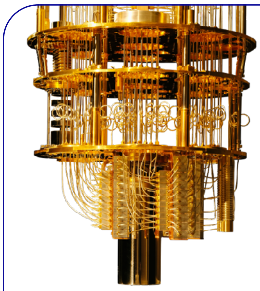
*The recommendations presented in this booklet, made by French experts from Campus Cyber members and experts from the Netherlands, will give you a better understanding of the issues at stake and the resources that must be put in place to ensure the security of our data and, more broadly, the security of our citizens.*

*Thank you, and enjoy your reading.*

Michel Van den Berghe
President - Campus Cyber

# < THE QUANTUM THREAT >

## A SYSTEMIC SECURITY CHALLENGE



**Efficient quantum computers** will be capable of weakening symmetric cryptographic algorithms and breaking the most commonly used asymmetric cryptographic ones. Such a computer would **call into question the foundations** on which the **security** of the Internet and our IT/OT infrastructures are based.

In practice, public-key algorithms are present in many systems.

This means that the **security** of most of the **digital services and infrastructures** we use is **threatened with collapse,** for example:

Secure Internet · VPN · Apps · Blockchain · Identities · IoT · Signature · Payments

**All public and private organizations are concerned, and will have to carry out plans for transforming and migrating their IT/OT infrastructures towards solutions resistant to quantum attacks.**

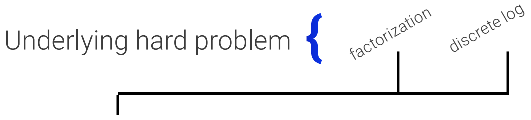
**Symmetric (secret-key)** algorithms are often used in **combination** with **asymmetric** (public-key) algorithms (for example: in the authenticated exchange of secret keys).

Deploying **quantum-safe** symmetric algorithms only makes sense if the asymmetric algorithms used with them are also resistant to quantum attacks.

### ASYMMETRIC CRYPTOGRAPHY (PUBLIC-KEY) AND ALGORITHMS AT RISK

All the most widely deployed **public-key algorithms** (based on two major mathematical problems: discrete logarithm and factorization) are **vulnerable** to quantum computers.

| FUNCTION | PROPERTY | ALGORITHMS | |
|---|---|---|---|
| Encryption | Confidentiality | RSA | ElGamal |
| Signature | Authentication | RSA | ECDSA |
| Key exchange | Secret key agreement | RSA | ECDH |



Underlying hard problem {

Resolution of mathematical problemes with Shor's quantum algorithm = **collapsing of mentionned public-key algorithm**

### SYMMETRIC-KEY CRYPTOGRAPHY (SECRET KEY) NOT STRUCTURALLY THREATENED

**Symmetric-key** (or secret-key) **algorithms** are less affected by quantum attacks (Grover's algorithm and its variants). While the actual cost of Grover's algorithm is debatable, the most reasonable option for protecting against it is to **double the key size**.

| FUNCTION | PRE-QUANTUM | POST-QUANTUM |
|---|---|---|
| Encryption | AES 128 | AES 256 |
| Hash | SHA-256 | SHA-384, SHA-512 |

# < THE QUANTUM THREAT >

## WHY DO WE NEED TO TAKE ACTION NOW?

Beyond expert estimates of when a sufficiently powerful quantum computer (CRQC, Cryptographically Relevant Quantum Computer) will arrive - 2030, 2035, 2040 or later - **the risk and its impact** are considered by security agencies **to be high**, and some data is already affected by the threat. So we need to act now and **prepare for the transition to quantum safe solutuions.**

NIST National Institute of Standards and Technology U.S. Department of Commerce

> " QUANTUM RISK IS NOW SIMPLY TOO HIGH AND CAN NO LONGER BE IGNORED "

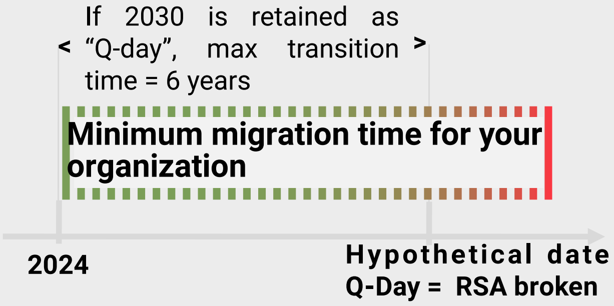
## « STORE NOW, DECRYPT LATER » – SENSITIVE, LONG-LASTING DATA IS ALREADY AT RISK

Some organizations have the capacity to massively **collect** and store our communications and data, aiming to **decrypt** them when a sufficiently powerful quantum computer becomes available. **Long-term secret data** is already concerned.

**"ANSSI recommends introducing post-quantum defense-in-depth as soon as possible for security products aimed at offering long-lasting protection of information (until after 2030) "** [1]

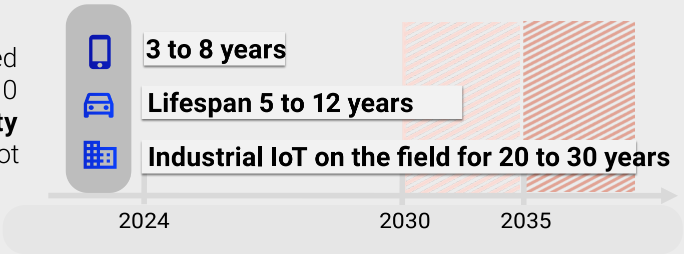
## TIME TO MIGRATE TO QUANTUM-RESISTANT INFRASTRUCTURES MUST BE ANTICIPATED

We need to be ready for the day when a sufficiently powerful quantum computer exists. Migration to post-quantum cryptography will take several years (5-10) for a typical large company. We need to **be prepared** and **anticipate** this transition time.


If 2030 is retained as "Q-day", max transition time = 6 years
Minimum migration time for your organization
2024
Hypothetical date Q-Day = RSA broken

## THE LIFE CYCLE OF IT SYSTEMS AND PRODUCTS MUST BE TAKEN INTO ACCOUNT

Some IT systems or embedded products are deployed in the field for **long periods**, sometimes 20 to 30 years in the case of industrial **IoT**, **without the ability to update** the underlying cryptography if this has not been anticipated.



[1] Please refer to ANSSI's position paper: "Views on the Post-Quantum Cryptography"

# < THE SOLUTION >

## POST-QUANTUM CRYPTOGRAPHY

### POST-QUANTUM CRYPTOGRAPHY PRINCIPLES

The **most widely deployed public-key algorithms** are based on mathematical problems (discrete logarithm, factoring) that can be solved with **Shor's quantum algorithm.**

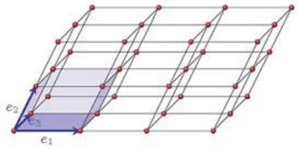
The algorithms currently in use are therefore no guarantee of security against a quantum computer.

Shor's algorithm is so effective that simply increasing the size of asymmetric keys is not a solution. To be resistant to this attack, for example, we would have to use RSA keys of 1 terabyte (instead of the current 384 bytes), which is totally impracticale.

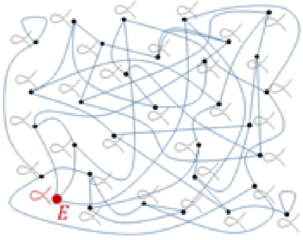
**Remediation** consists in using public-key algorithms based on different **mathematical problems**, which cannot be solved in practice with a quantum computer: these are **post-quantum or quantum-resistant algorithms.**

Post-quantum public-key algorithms provide **similar functionality** to classical algorithms, and are destined to be **deployed on today's computing infrastructures** in response to this threat created by quantum computing.

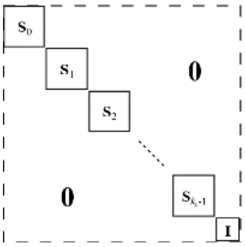
### UNDERLYING MATHEMATICAL PROBLEMS



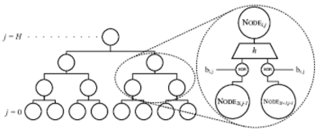
Euclidean lattices (frontrunner)



Isogeny (outsider)



Error-correcting codes (conservative)



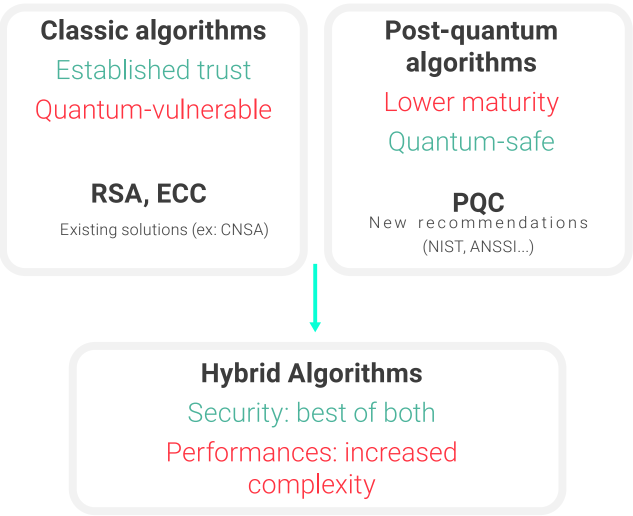
Symmetric crypto functions (conservative)

$$p^{(1)}(x_1,\dots,x_n)=\sum_{i=1}^{n}\sum_{j=i}^{n}p_{ij}^{(1)}\cdot x_ix_j \;+\; \sum_{i=1}^{n}p_i^{(1)}\cdot x_i+p_0^{(1)}$$
$$\vdots$$
$$p^{(m)}(x_1,\dots,x_n)=\sum_{i=1}^{n}\sum_{j=i}^{n}p_{ij}^{(m)}\cdot x_ix_j \;+\; \sum_{i=1}^{n}p_i^{(m)}\cdot x_i+p_0^{(m)}$$

Multivariate equations (outsider)

### HYBRIDIZATION: CLASSICAL + POST-QUANTUM

**Hybridization** aims to **combine pre-quantum cryptographic algorithms with post-quantum algorithms** in protocols, **to guarantee maintaining existing security levels** while preparing for **future threats.**



**Classic algorithms**

Established trust

Quantum-vulnerable

**RSA, ECC**

Existing solutions (ex: CNSA)

**Post-quantum algorithms**

Lower maturity

Quantum-safe

**PQC**

New recommendations (NIST, ANSSI...)

**Hybrid Algorithms**

Security: best of both

Performances: increased complexity

### COMMUNICATION PROTOCOLS

🔒 | https:// → TLS post-quantum hybrid

Post-quantum algorithms must be implemented in standardized communication protocols and commonly used cryptographic mechanisms.

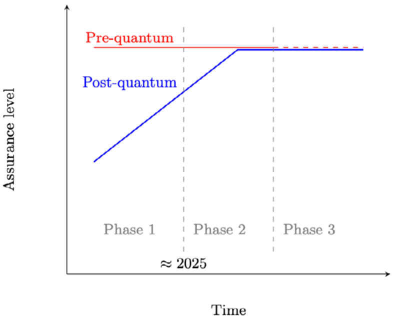
This has **an impact on our day-to-day activities:** visiting a secure website, sending an email, making a credit card payment, signing a document, authenticating an identity...

**Deploying post-quantum algorithms** requires a minimum of **adaptation** (encryption algorithms, digital signatures). In some cases, a **simple drop-in algorithm replacement is not possible** (Diffie-Hellman key exchange) and a **major overhaul of protocols** is needed.

# < NATIONAL AGENCIES BOOST TRANSITION >

The national security agencies are positioning themselves and gradually providing their recommendations for methods and timetables.

Federal Office for Information Security

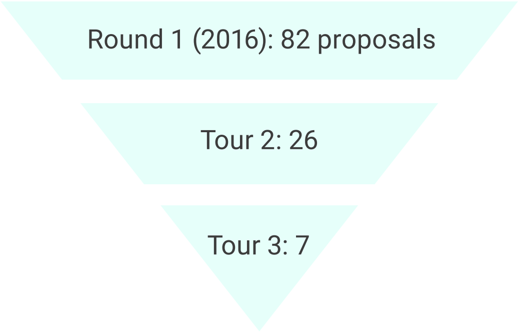


- We must rely on the NIST ongoing processes of selection of **new algorithms**, widely **studied** by the scientific community;
- The **ANSSI** in France and the BSI in Germany support the NIST approach in the USA, but also make **their own recommendations**, such as the use of FrodoKEM algorithm;
- **Hybrid protocols** are the **only recommended mode** (in Europe) of implementing post-quantum public key cryptography.
- From **2024-2025**, **post-quantum security visas** may be issued;
- From the same date, hybrid cryptography **may be mandatory** in certain contexts.

## US NIST STANDARDIZATION PROCESS

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST (the U.S. National Institute of Standards and Technology) launched a process in 2016 to select new algorithms as standards for post-quantum cryptography, engaging the global cryptographic community.



Round 1 (2016): 82 proposals

Tour 2: 26

Tour 3: 7

**First selections in July 2022**

CRYSTALS-KYBER /

CRYSTALS-DILITHIUM / FALCON / SPHINCS+

Other countries, such as China and South Korea, have organized their own processes and choices of post-quantum algorithms.

## THE UNITED STATES IN ACTION TO RESPOND TO THE THREAT AND SET UP AN ADVANCED ECOSYSTEM

- **NIST** (July 2022): **first selection of post-quantum algorithms.**
- **NCCoE** (July 2022): launch of the **"Migration to PQC"** initiative with 20 manufacturers.
- **NSA** (September 2022): update of the cryptographic **reference document for National Security Systems.**
- **White House** (November 2022): publication of Memorandum NSM-10 (and passage of a bill in Congress), instructing federal agencies to **launch the transition: inventory, definition of transition plans, conducting** pilots in production before standards are finalized, implementation of governance and centralized reporting, with the first milestone in May 2023.
- **Homeland Security Department** (October 2022): announcement of a migration target for their critical systems by 2030.
- **New National Cybersecurity Strategy** (March 2023): PQC is treated as part of the "Invest in a resilient future" pillar.

At the heart of many industrial issues, cross-functional standards organizations (IETF, ETSI, ITU, ISO/IEC, IEEE...) and industry-specific organizations (GSMA, EMVCo...) have active working groups to define up-to-date standards.

# < ACTIONS TO BE TAKEN >

**Migration** to quantum-safe infrastructures in a **highly connected and interoperable ecosystem** represents an **unprecedented transformation challenge.**

In practice, every organization needs to **integrate the quantum threat** into its major risk mapping, and embark on the path of **transition** with an overall medium-term vision of 5 to s10 years, and actions that can be triggered today.

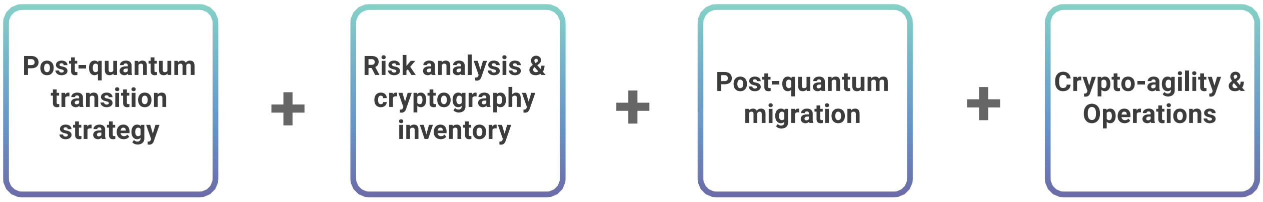
## KEY ACTIONS TO PREPARE YOURSELF

- **Raising awareness** about the quantum threat and the ways to be prepared;
- **Cryptographic inventory** to map the underlying cryptography;
- **Pilots** to test technical solutions on use cases, understand migration issues and build a coherent, global transition strategy;
- **Crypto-agility:** understand the challenges of crypto-agility at different levels (algorithms, protocols, systems, end-to-end use cases) and integrate crypto-agility to prepare for the arrival of post-quantum hybrid cryptography;
- **Purchasing policy:** integrate the post-quantum dimension into specifications for IT solutions (HSM, PKI, communication applications, business software, IoT and embedded systems, etc.).

## GLOBAL VISION: THE POST-QUANTUM TRANSITION ROADMAP

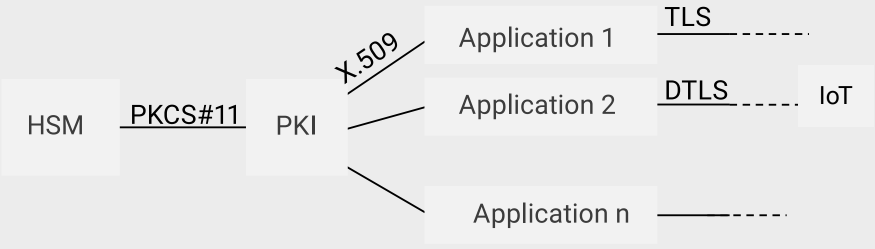
All public and private organizations will have to:

1. **define** post-quantum transition plans, including **cryptographic inventories, critical data** mapping and **prioritization;**
2. **migrate** to quantum-resistant infrastructures or embedded products;
3. **set up** an organization and **crypto-agile solutions** for conducting operations, and facilitate **the application of the latest recommendations.**


Post-quantum transition strategy
+
Risk analysis & cryptography inventory
+
Post-quantum migration
+
Crypto-agility & Operations

## CONCRETE MIGRATION CHALLENGES IN AN INTEROPERABLE ENVIRONMENT

For example, in large organisations, **end-to-end use cases very often involve various components** such as PKIs to produce certificates, applications that use these certificates or applications connected to Internet via TLS protocols. The challenge is **to manage this transition** while ensuring the **coherence, interconnection and end-to-end interopeability** of the components involved.



# < Studio des Communs >

A COLLABORATIVE DOCUMENT PRODUCED BY THE PQC - AWARENESS WORKGROUP, OF WHICH THE FOLLOWING ENTITIES ARE MEMBERS:

CRYPTONEXT SECURITY

Inria

orange™

HeadMind Partner

i-TRACING CYBERSECURITY

AIRFRANCE

eDF

AXA

CAMPUS CYBER

MORE INFORMATION: WWW.WIKI.CAMPUSCYBER.FR
CONTACT: COMMUNAUTES@CAMPUSCYBER.FR / 5 - 7 RUE BELLINI 92800, PUTEAUX