X-SPIErience Day 2020

SOUVERAINETÉ NUMÉRIQUE

SPIE

cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

X-SPIErience Day 2026
SOUVERAINETÉ NUMÉRIQUE

SPIE

Garantir la souveraineté des données en adoptant la cryptographie résistante aux ordinateurs quantiques

FRÉDÉRIC NOYER

Head of Governance Services & Pentesting
SPIE ICS

C1 – PUBLIC

SPIE, sharing a vision for the future

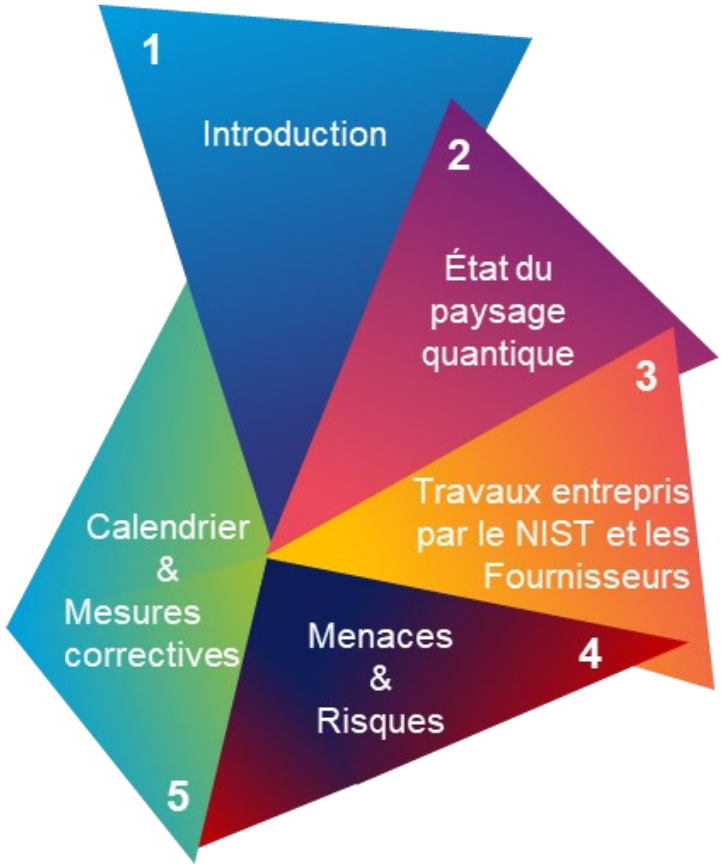
Protection de la souveraineté à l'ère quantique

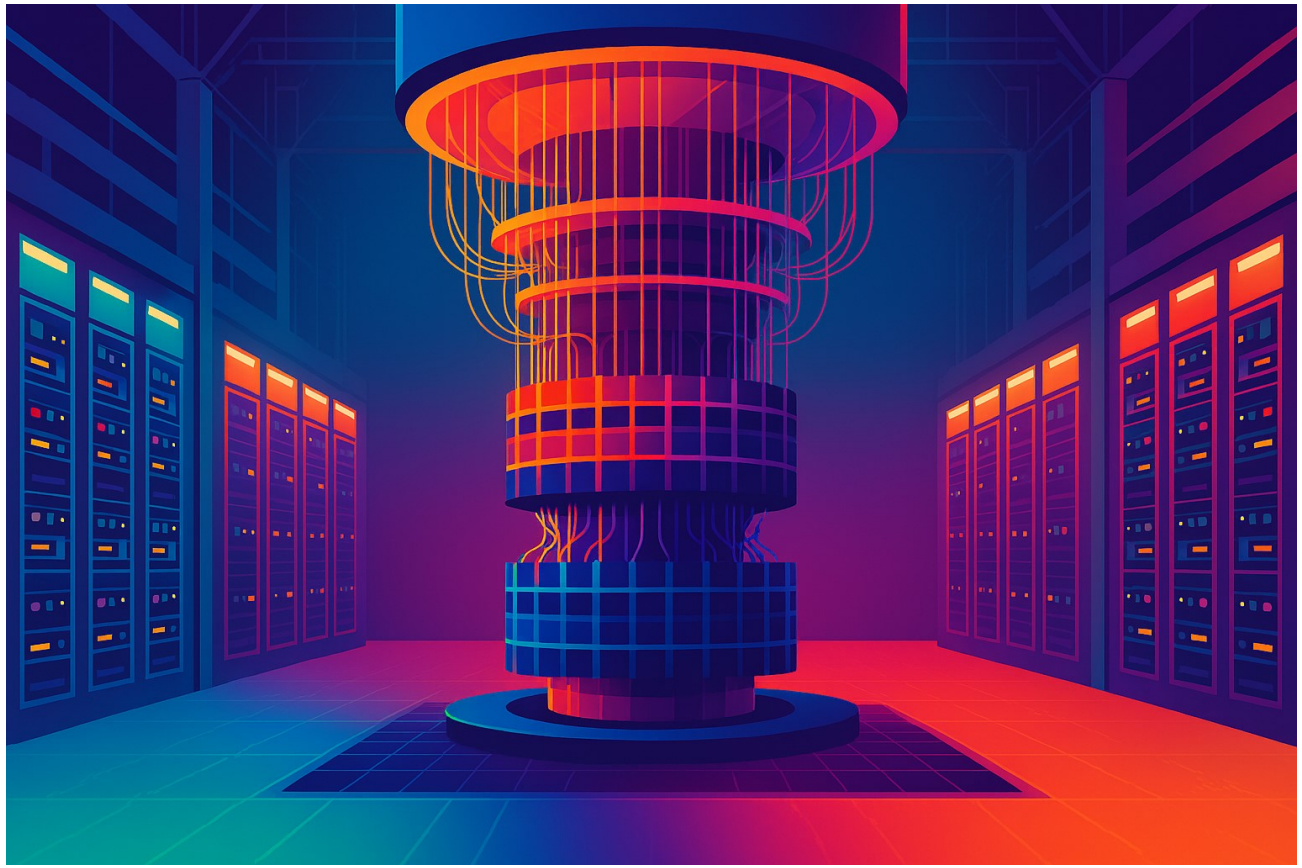
« La **souveraineté numérique**, c'est la **capacité d'un État ou d'une organisation à contrôler ses propres données et infrastructures numériques**.

Aujourd'hui, avec **l'avènement de l'informatique quantique**, **la menace plane sur la confidentialité et l'intégrité des communications** car la cryptographie classique est à risque.

Se **préparer à la transition vers la cryptographie quantique** devient ainsi un **enjeu central** pour **préserver notre autonomie et notre indépendance numérique**. »

Agenda





L'utilisation de l'IA a permis la génération d'images présentes dans cette présentation.

Cette présentation a pour objectif de vous informer sur la transition vers des algorithmes PQC.

Définitions

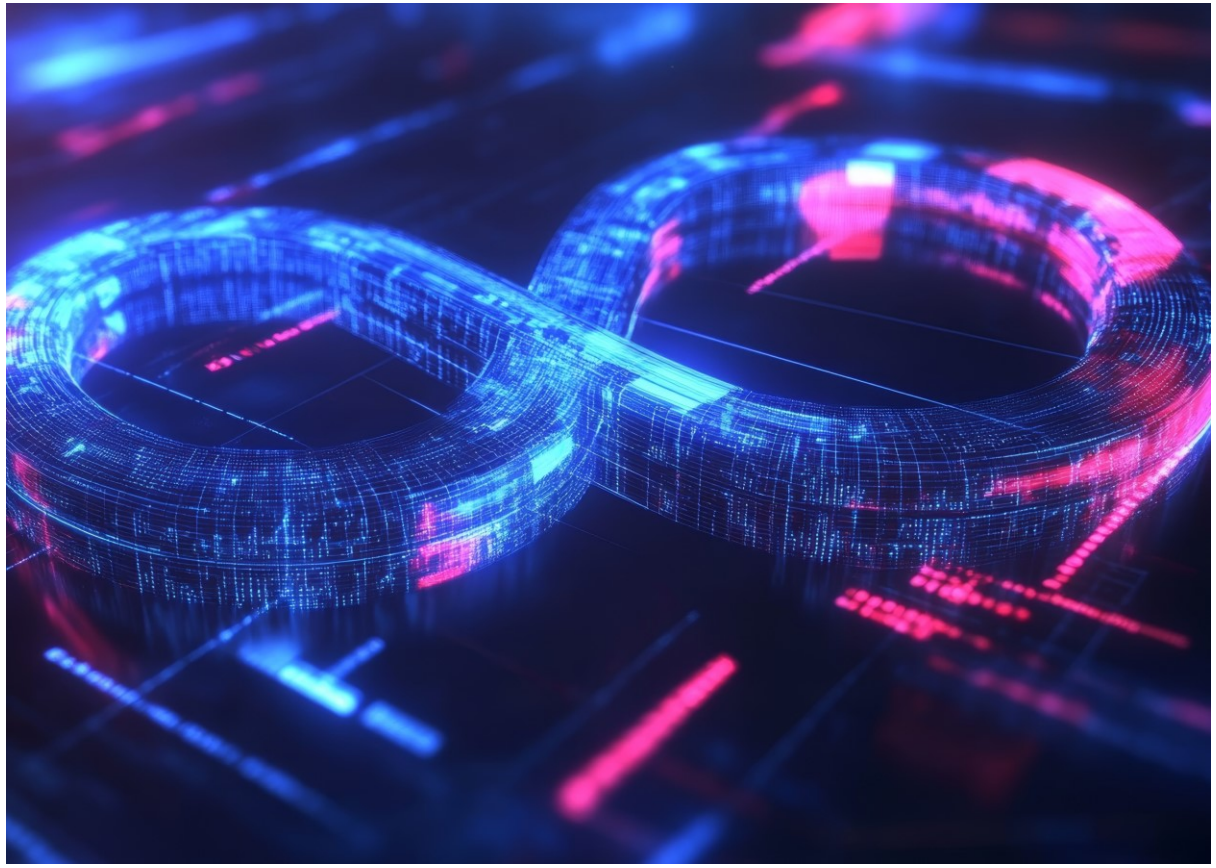
Qu’est-ce que PQC ?

La PQC (**Post-Quantum Cryptography** ou cryptographie post-quantique) désigne une branche de la cryptographie qui se concentre sur le développement d’**algorithmes de chiffrement résistants aux attaques des ordinateurs quantiques**.

Ces **algorithmes sont conçus pour garantir la sécurité des données et des communications** même dans un monde post-quantique, où des ordinateurs quantiques puissants pourraient exister.

Qu’est-ce que la Crypto-Agilité ?

La **crypto-agilité** désigne la capacité d’un système informatique à **modifier rapidement et facilement ses algorithmes ou protocoles cryptographiques** en réponse à de nouvelles menaces ou évolutions technologiques, **sans grands efforts** techniques.



Durée de vie des certificats

Avant 2012 → **10 ans**

2012 → **5 ans**

2015 →**3 ans**

2018 → **2 ans**

2020 → **398 jours**

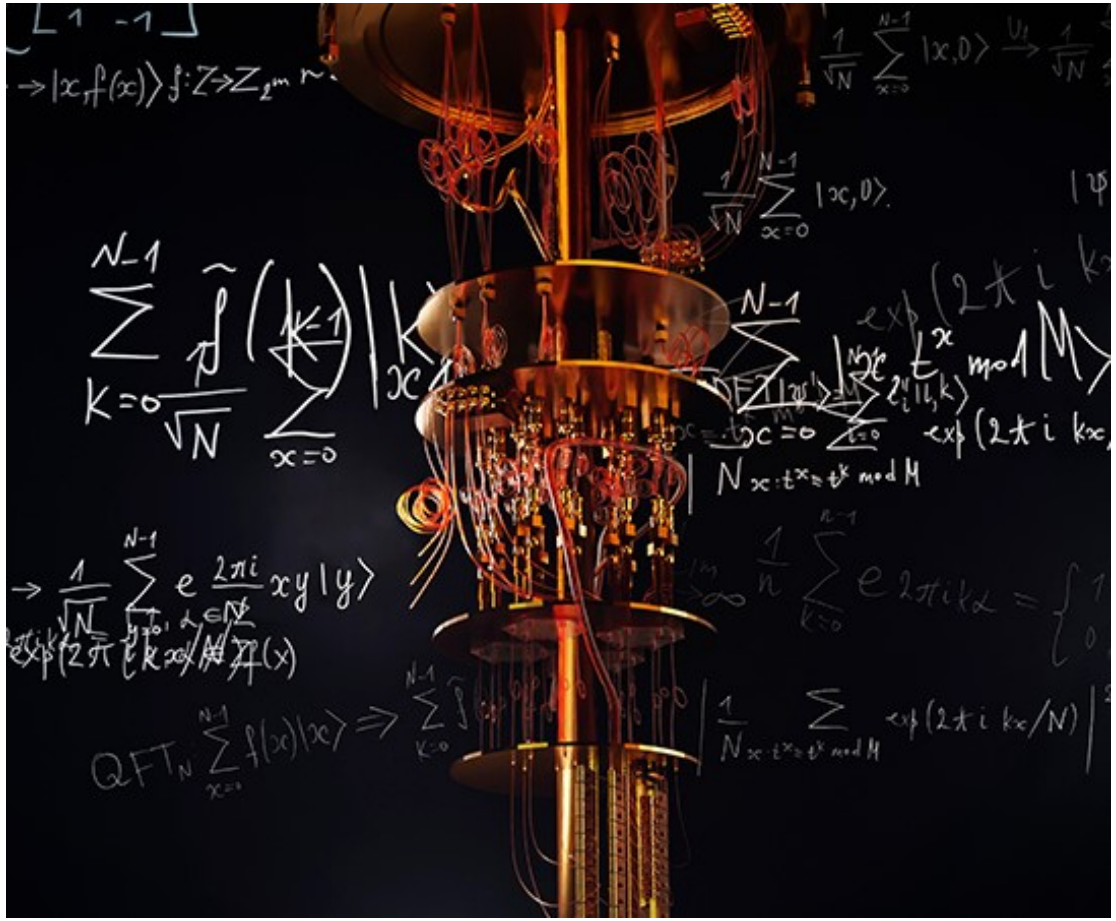
2026 → **200 jours**

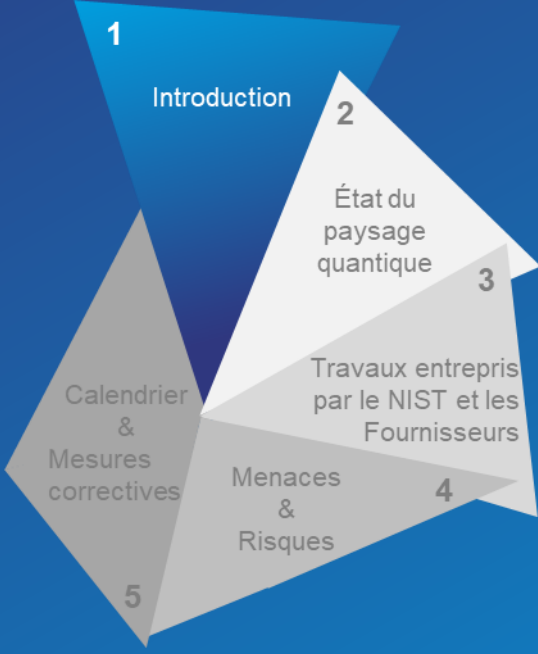
2027 → **100 jours**

2029 → **47 jours**

Qu’est-ce que le “Q-Day“ ?

Le terme “**Q-Day**“ (ou “**Quantum Day**”) désigne le jour hypothétique où un ordinateur quantique à grande échelle et tolérant aux fautes deviendra capable de casser les algorithmes de cryptographie.





Introduction

Un ultimatum comme point de départ

C'EST LA PREMIÈRE FOIS DANS L'HISTOIRE QUE L'ON CONNAÎT À L'AVANCE UNE

ZERO DAY

Retour sur l'histoire

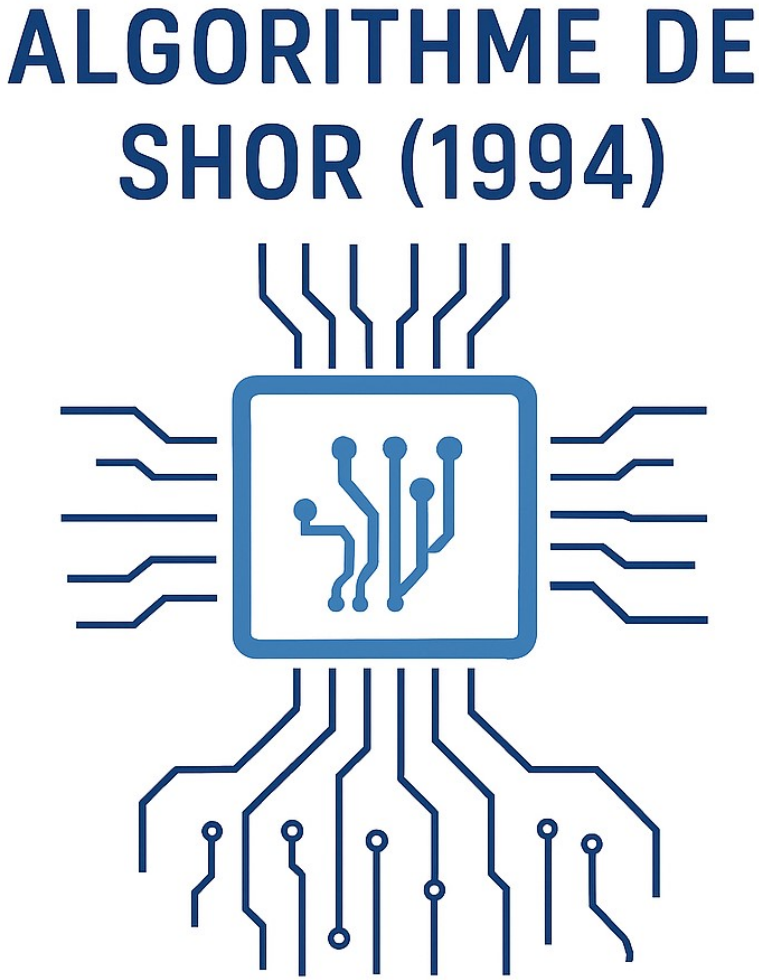
Algorithme de Shor (1994) :
Peut résoudre le problème du logarithme discret

Implication: Compromet

Diffie-Hellman (DH)

Cryptographie à courbes elliptiques (EC)

RSA (factorisation des nombres composés).



Retour sur l'histoire

Algorithme de Grover (1996) :
Permet de rechercher dans une base de données non triée de N éléments en temps $O(\sqrt{N})$

Implication: Réduction de la sécurité des chiffrements symétriques d'un facteur 2 (comme AES).

Impact sur la sécurité de nos systèmes

Confidentialité

Encryption

- AES
- Key Agreement
- Diffie-Hellman

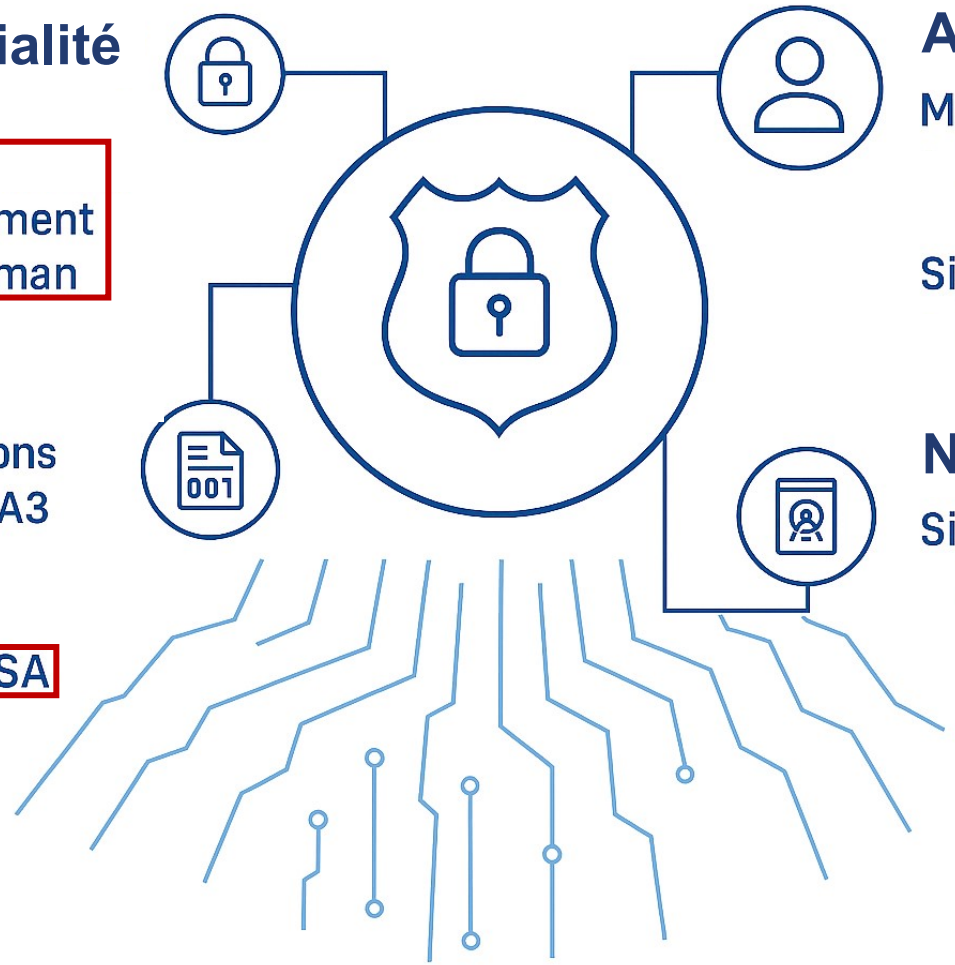
Intégrité

Hash Functions

- SHA-2, SHA3
- SHAKE

Signatures

- RSA/ECDSA



Authenticité

MACs

- HMAC
- GMAC/CMAC

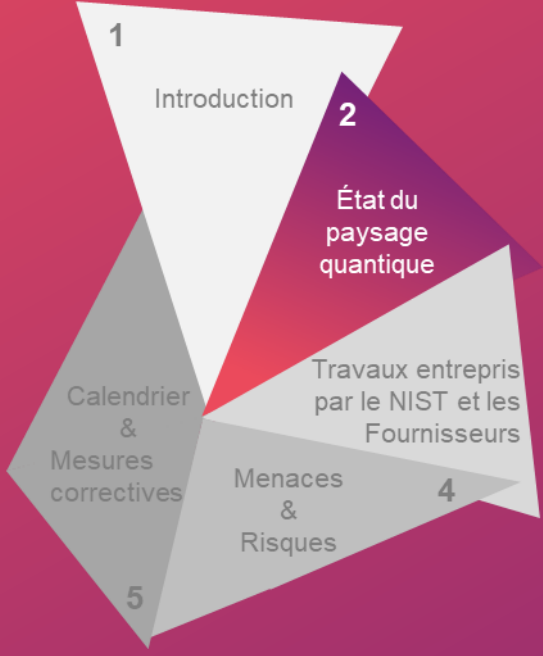
Signatures

- RSA/ECDSA

Non-Répudiation

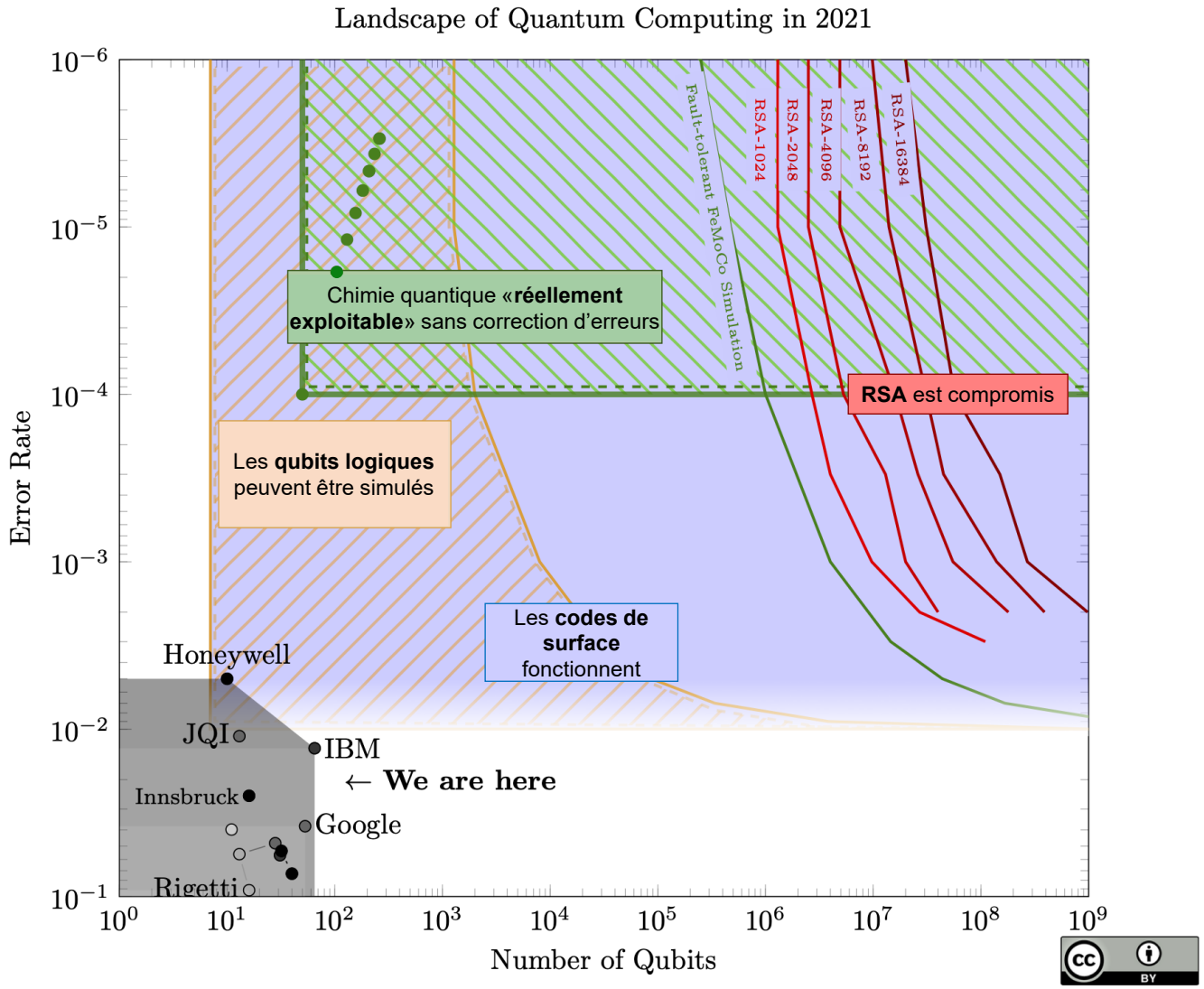
Signatures

- RSA/ECDSA



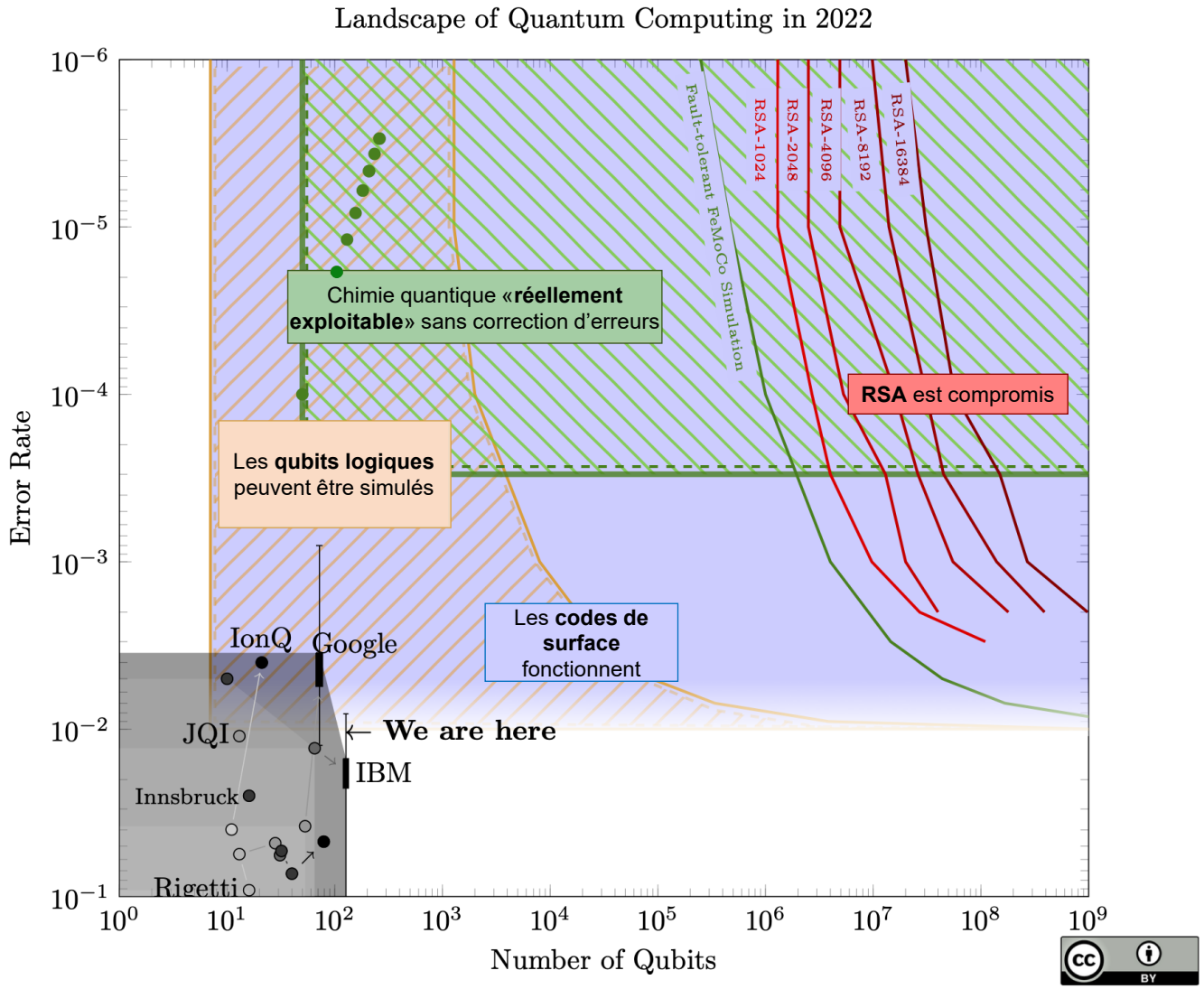
État du paysage quantique

Paysage de l'informatique quantique



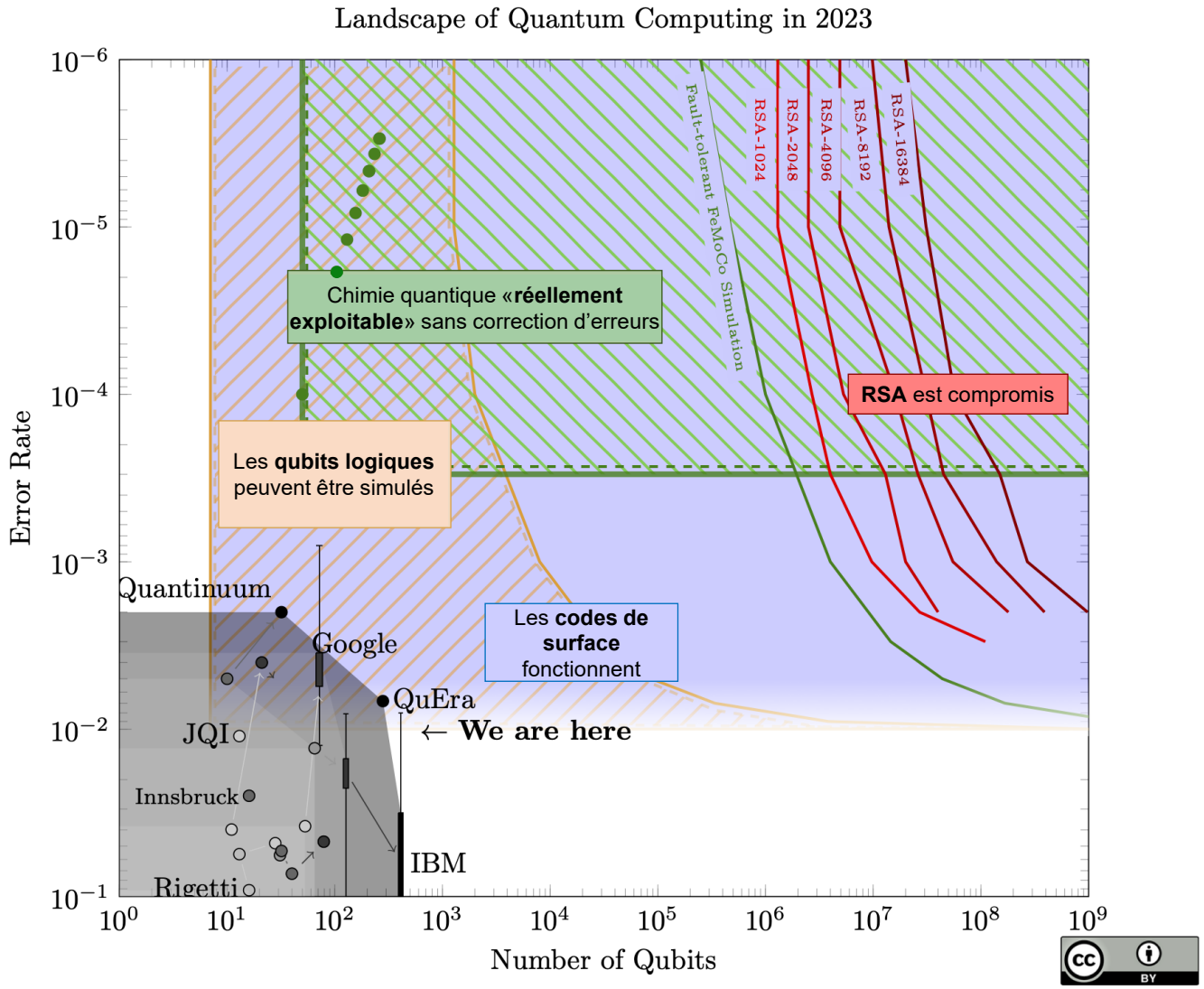
sources: https://sam-jaques.appspot.com/quantum_landscape

Paysage de l'informatique quantique



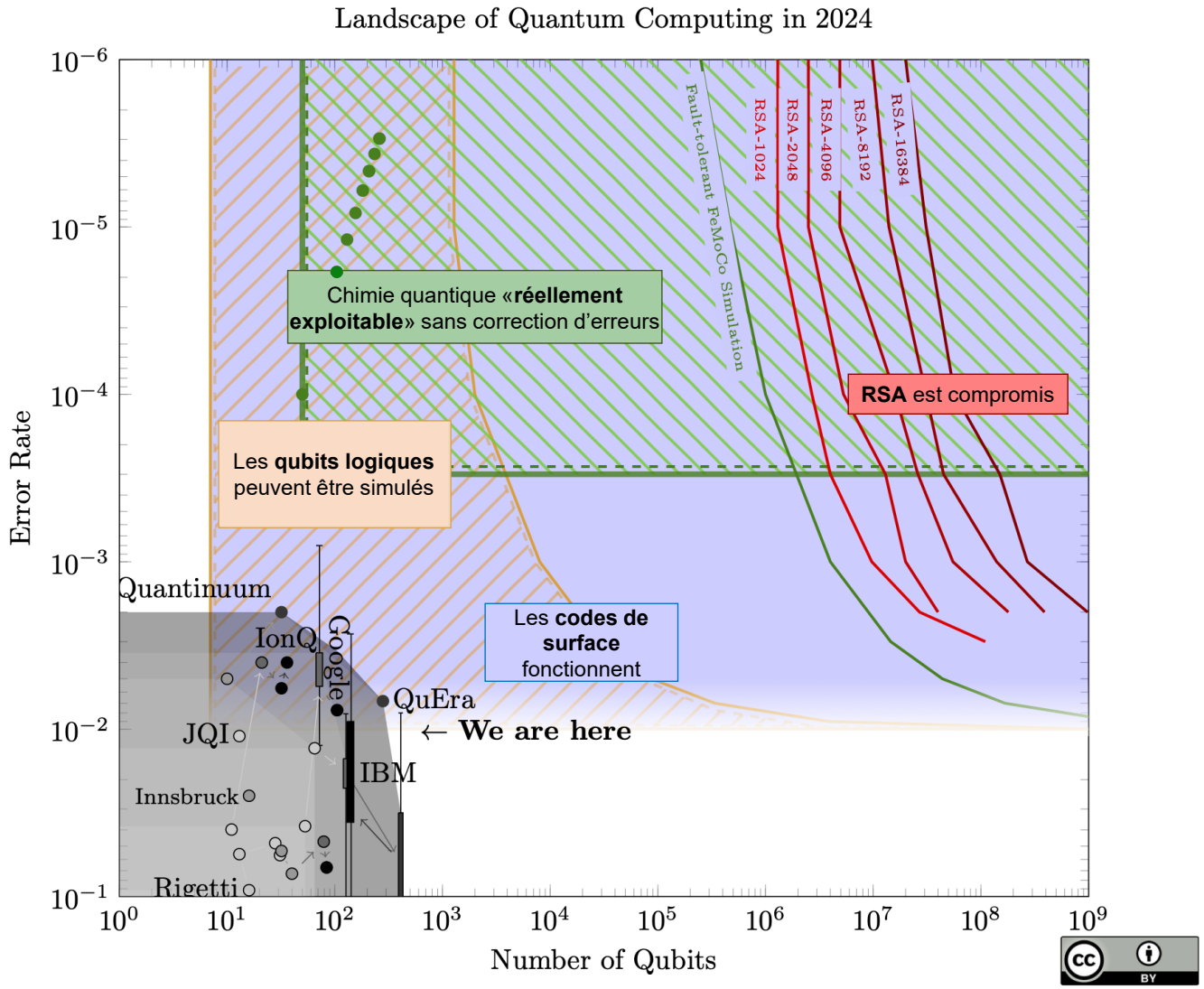
sources: https://sam-jaques.appspot.com/quantum_landscape

Paysage de l'informatique quantique



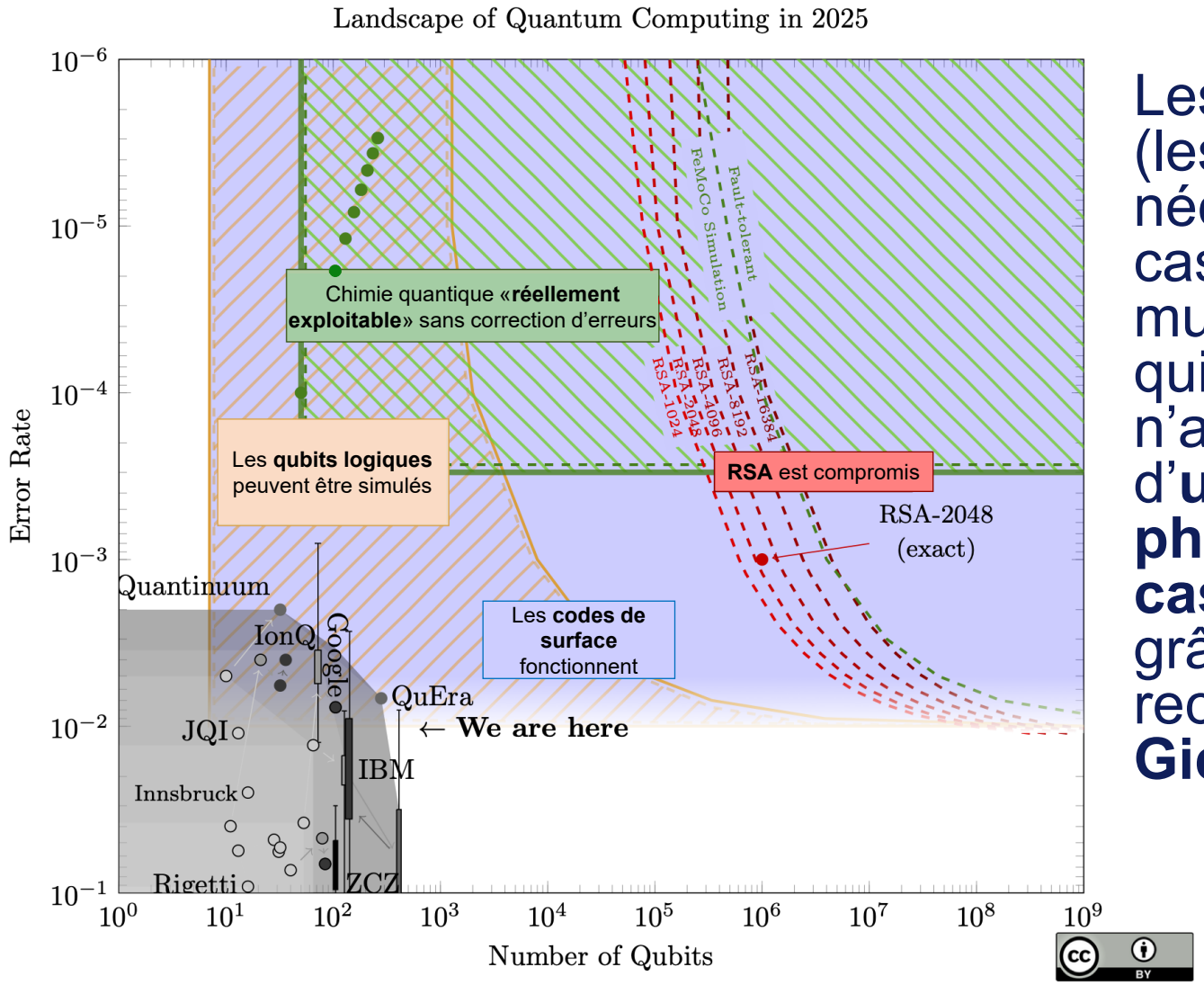
sources: https://sam-jaques.appspot.com/quantum_landscape

Paysage de l'informatique quantique



sources: https://sam-jaques.appspot.com/quantum_landscape

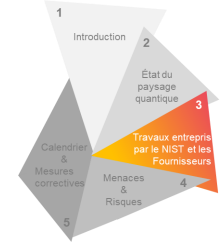
Paysage de l'informatique quantique



Les courbes de droite (les ressources nécessaires pour casser RSA) ont été multipliées par 20, ce qui signifie que nous n'avons besoin que d'**un million de qubits physiques pour casser RSA-2048**, grâce au résultat de la recherche de **Craig Gidney**.

sources: https://sam-jaques.appspot.com/quantum_landscape

Travaux entrepris par le NIST et les Fournisseurs



Initiative du NIST

69 soumissions répondent aux exigences spécifiées

Début du premier tour

2017

2018 – Le deuxième tour commence avec 26 candidats restants

2019 – Le troisième tour commence avec 15 candidats restants

2018 - 2019

Le **NIST publie 3 projets** de normes pour consultation publique

Le NIST annonce un appel à contributions pour des algorithmes de signature numérique supplémentaires

Le quatrième tour se poursuit

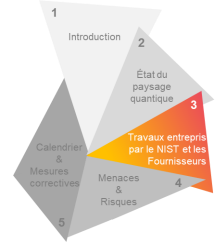
2023

Le **NIST publie les premiers algorithmes PQC**

Début du premier tour pour les signatures numériques additionnelles

Le quatrième tour se poursuit

2024



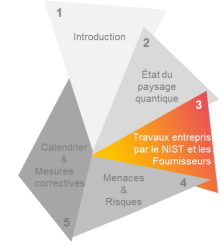
Quels sont ces nouveaux algorithmes - NIST PQC Standards

FIPS 203: Module-Latice-Based Key-Encapsulation Mechanism Standard (**ML-KEM**)

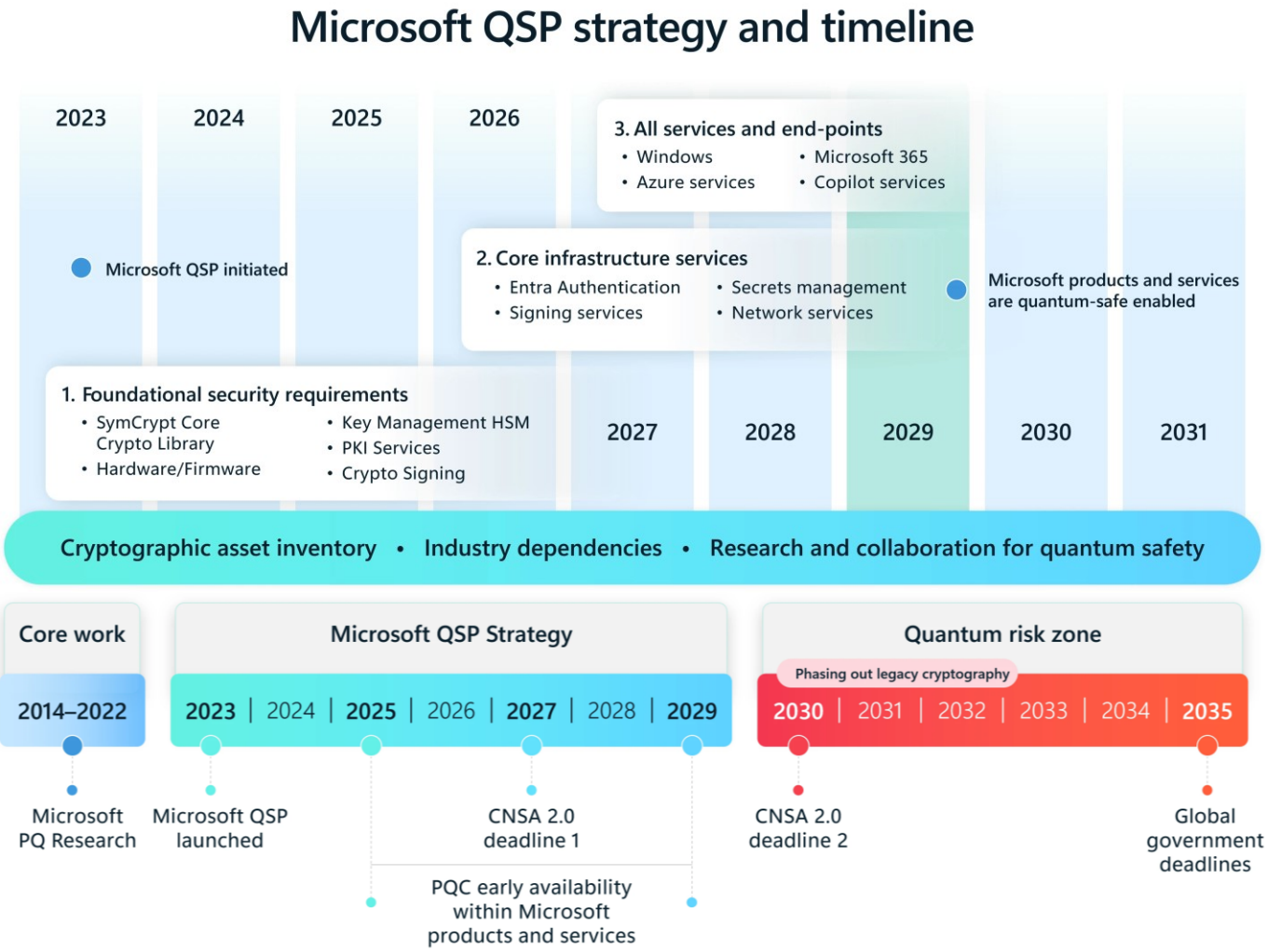
FIPS 204: Module-Latice-Based Digital Signature Standard (**ML-DSA**)

FIPS 205: Stateless Hash-Based Digital Signature Standard (**SLH-DSA**)

FIPS 206 est en cours de révision et pourrait devenir le quatrième algorithme validé en 2026



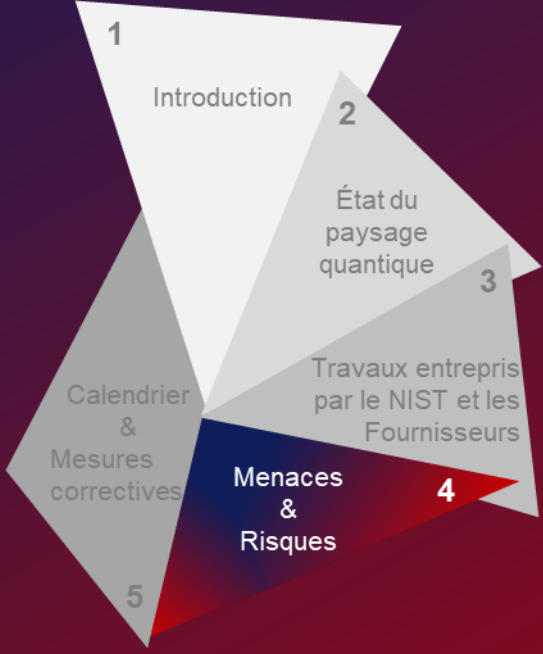
Roadmap type (exemple Microsoft)



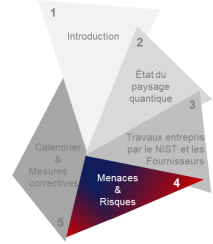
- 2025 : Microsoft **intègre ML-KEM** et **ML-DSA** à Windows Server 2025 et au client Windows

- 2025 : Microsoft annonce la disponibilité générale de la **prise en charge de PQC dans .NET 10**.

- 2026 : PQC dans les services de certificats Active Directory (ADCS). Microsoft annonce que la disponibilité générale des **fonctionnalités PQC dans les services de certificats Active Directory (ADCS)** est prévue pour début 2026.



Menaces & Risques



Les acteurs de menace

Cybercriminels

Etats ou **Groupe sponsorisés par des états**

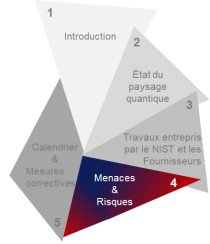
Hacktivistes

Initiés (internes)

Cyber-terroristes

Hackeurs Opportunistes

Compétiteurs

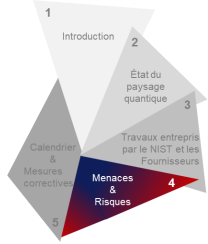


Les acteurs de menace liés à la PQC

Cybercriminels très organisés ou **consortiums criminels transnationaux**

Etats ou **Groupe sponsorisés par des états**

Compétiteurs (grandes entreprises technologiques)



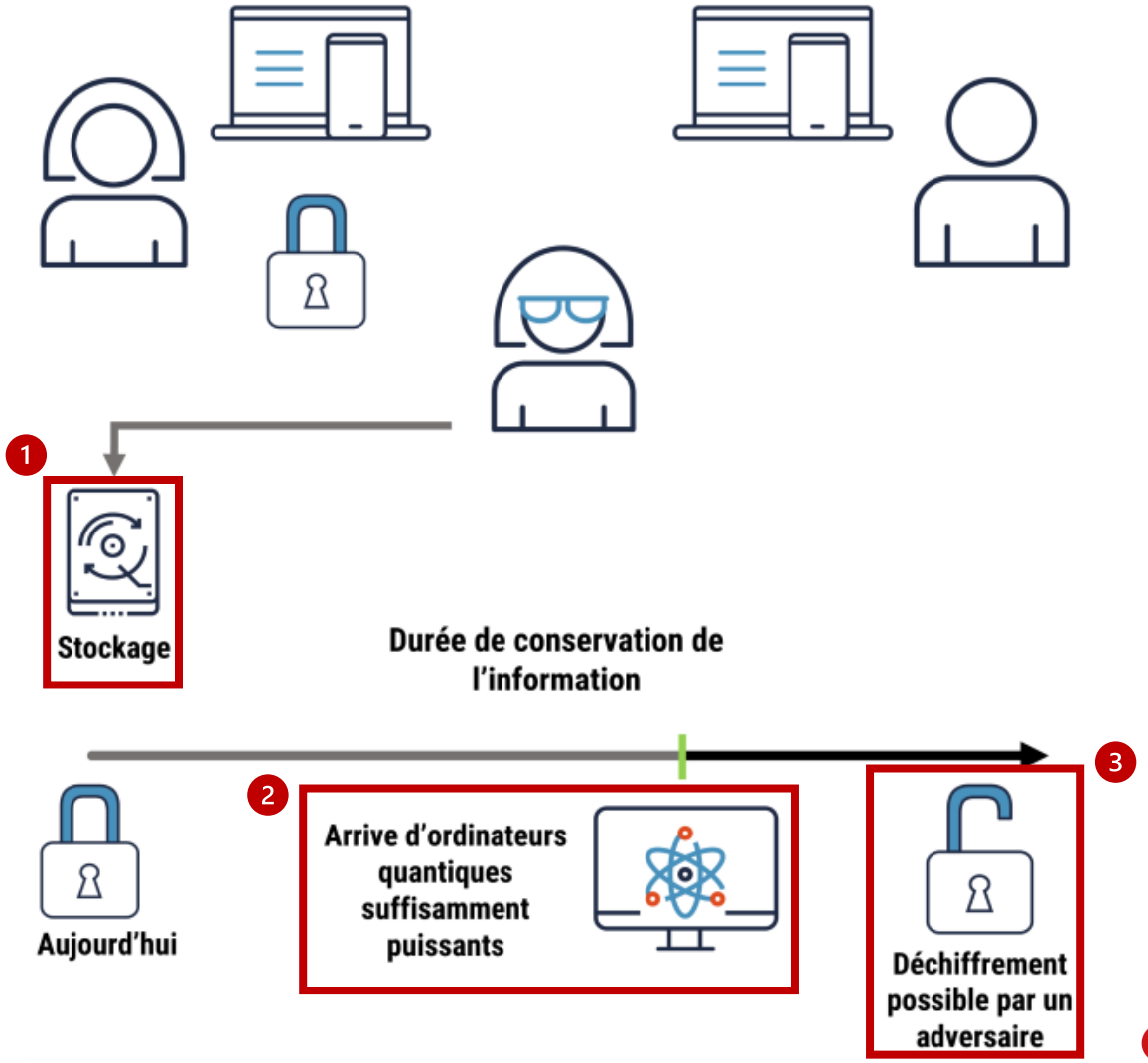
Risque: Harvest Now, Decrypt Later (HNDL)

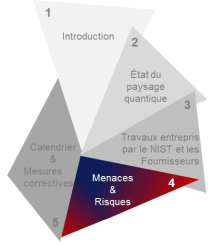
Des acteurs malveillants

1. **Volent, interceptent et stockent dès maintenant des informations chiffrées**, dans l'attente de
2. disposer à l'avenir d'un ordinateur quantique pour
3. **les déchiffrer rétroactivement**.

Les secrets compromis pourraient inclure :

- Propriété intellectuelle
- Informations stratégiques
- Données personnelles ou médicales sensibles

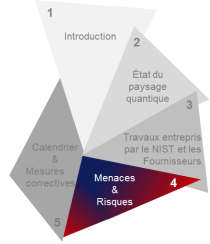




Non traitement du risque : « Le piège du report du risque quantique »

La gestion des **risques cryptographiques est souvent reléguée au second plan** en raison de sa nature perçue comme un processus à long terme, et est généralement reportée au RSSI suivant ou à la direction.

Cependant, les menaces émergentes telles que l'informatique quantique requièrent une **attention immédiate** afin d'éviter des conséquences catastrophiques à court terme.

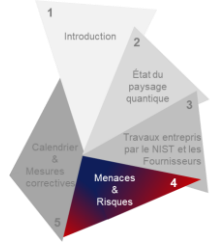


Non-conformité future

Le paysage international évolue rapidement : **l'Union européenne fixe des exigences de transition**.

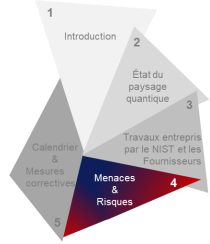
En Suisse, **les autorités alertent sur la nécessité d'anticiper la refonte cryptographique**.

Ignorer la préparation à cette transition expose les entreprises à un risque de non-conformité future.



Augmentation du cyber-espionnage étatique

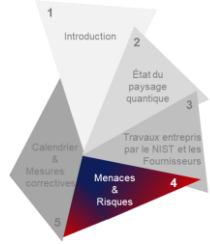
Des États pourront espionner massivement et rapidement des communications chiffrées d'autres pays, accélérant la course à l'armement cyber et l'instabilité géopolitique.



Risque fournisseur et perte de confiance dans les services numériques

Les certificats électroniques, signatures numériques et protocoles d'authentification deviennent vulnérables, menaçant l'intégrité :

- Des chaînes d'approvisionnement
- Des plateformes de vote électronique
- Des échanges bancaires et notariés
- …

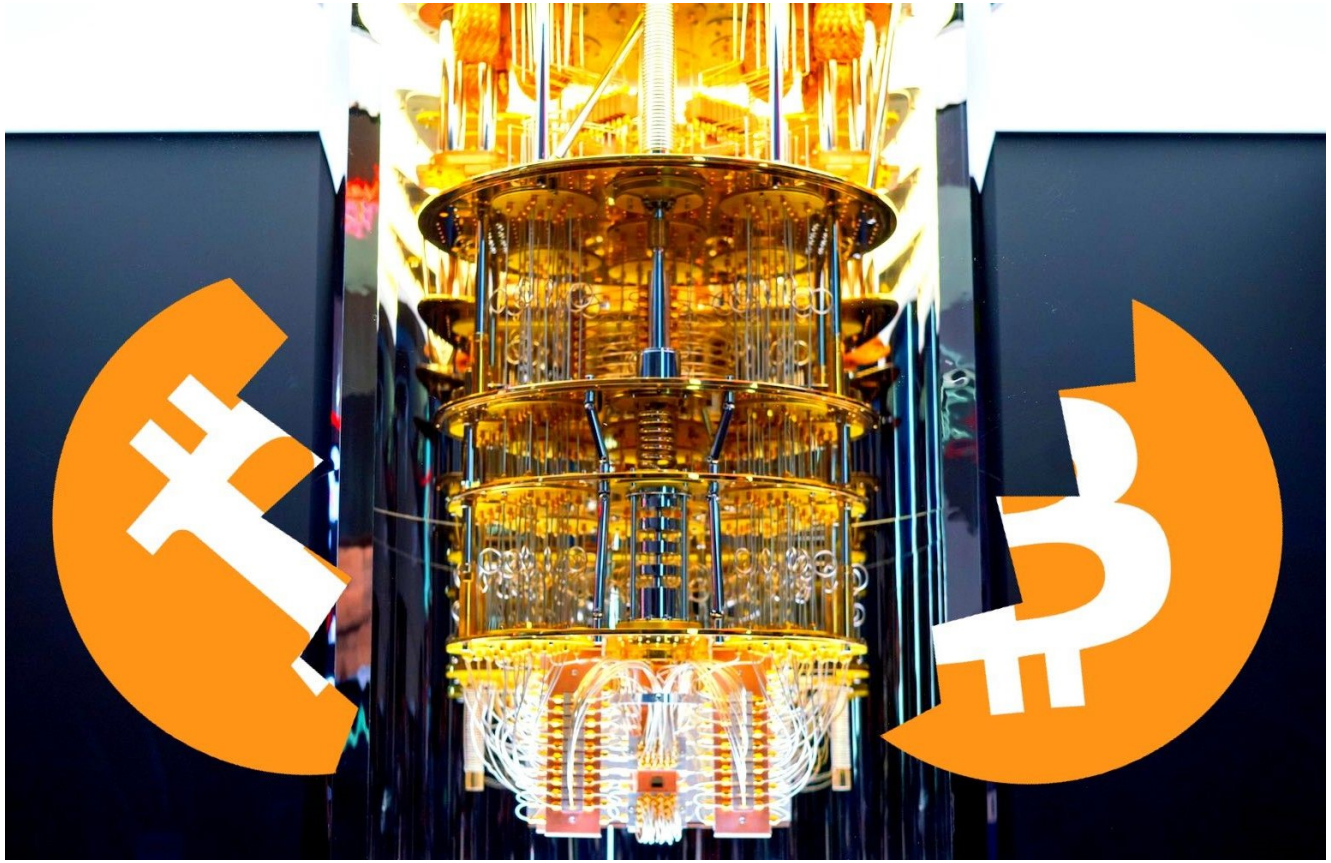


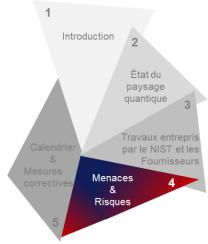
Intégrité de la blockchain à risque

Bitcoin et Ethereum utilisent tous deux **l'algorithme de signature numérique à courbe elliptique (ECDSA)**.

L'algorithme **ECDSA est vulnérable aux ordinateurs quantiques**, car l'algorithme de Shor peut résoudre efficacement les problèmes mathématiques sous-jacents.

Ceci permet aux attaquants de **falsifier les signatures et de compromettre le système**.



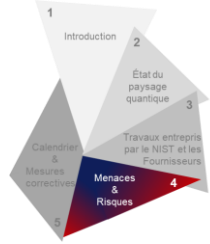


Risques pour l'identité numérique

Les ordinateurs quantiques représentent une **menace majeure pour la sécurité des identités électroniques modernes** (cartes d'identité, cartes de santé, passeports).

Ces documents reposent sur la cryptographie asymétrique (RSA, ECC), qui garantit aujourd'hui leur authenticité, l'intégrité des échanges et la protection des données personnelles.

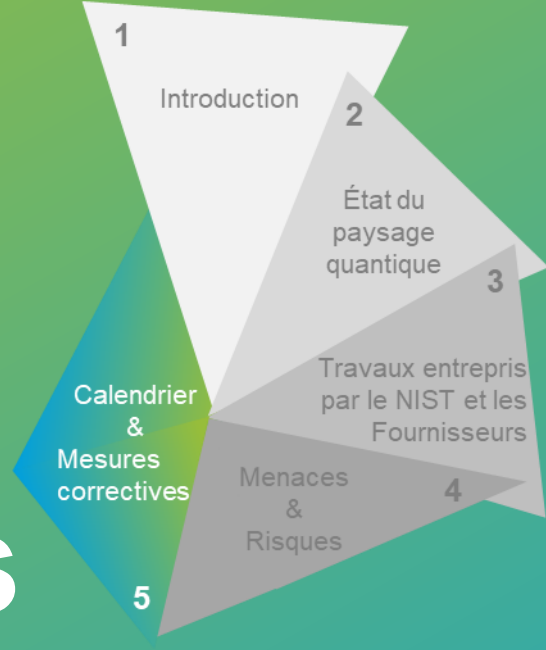
Il existe un risque réel (documenté par des experts et adopté comme priorité par la feuille de route UE) que les documents d'identité actuels deviennent fraudables et que des violations massives de vie privée deviennent possibles si la transition vers la cryptographie post-quantique n'est pas anticipée.



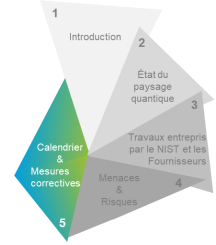
Risque de perturbation des infrastructures critiques

La compromission des communications de gestion et de contrôle :

- Les réseaux énergétiques, de transport, d'eau
- Les systèmes de commande industrielle (ICS/SCADA)
- Les infrastructures de santé

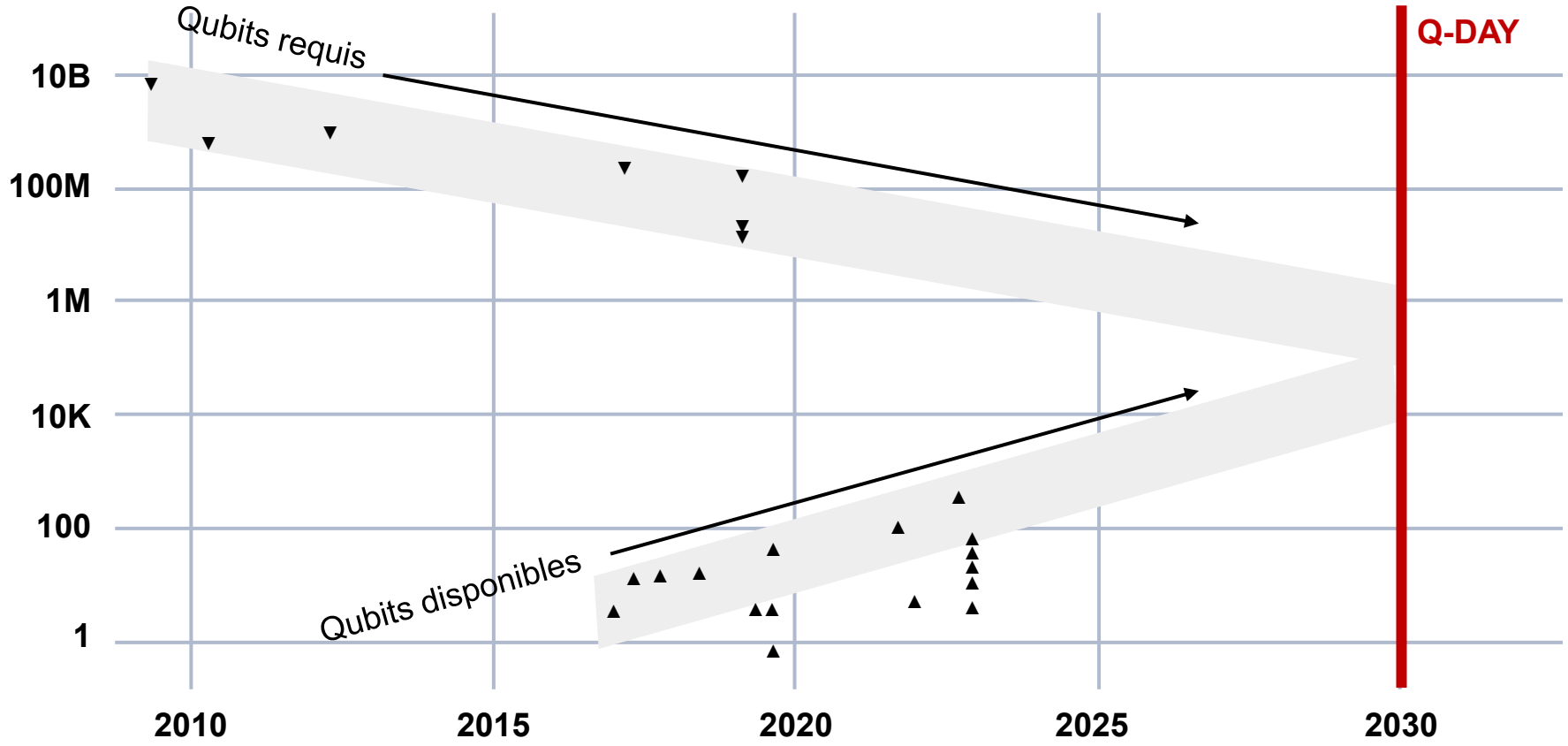


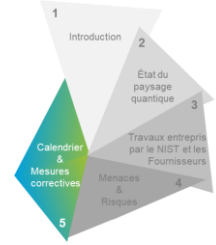
Calendrier et mesures correctives



Estimation de la « Q-DAY »

Le calendrier se précise, même si la date exacte reste inconnue.





SPIE vous accompagne dans cette transition

0 : **Révisez vos exigences** et **suivez le risque quantum**.

1 : Effectuez un **inventaire** de votre cryptographie.

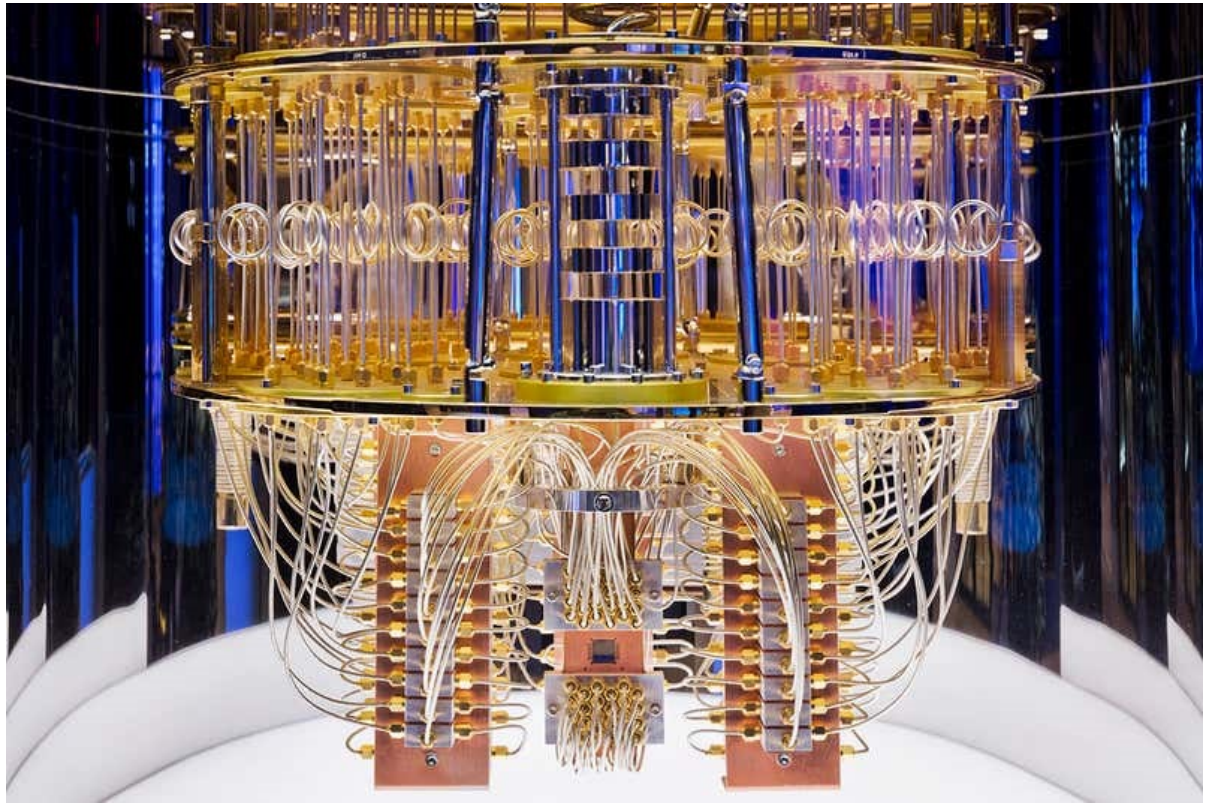
2 : Effectuez une **analyse de risque**, prioriser vos actions.

3 : Créez un **plan de migration**.

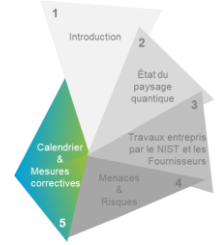
3.a : **Y inclure la chaîne d'approvisionnement/fournisseurs**

4 : **Utilisez la cryptographie post-quantique** et **doubler la taille des clés symétriques (AES).**

5 : **Modernisez votre PKI** et adopter la **crypto-agilité**.



N'hésitez pas à nous contacter en cas de question. Nous saurons vous accompagner dans vos défis!



En résumé

QUOI RETENIR

- La cryptographie classique est à risque
- L'utilisation de nouveaux algorithmes de chiffrement est inévitable
- La durée des certificats est raccourcie progressivement pour atteindre 47 jours en 2029
- L'automatisation et une préparation adéquate doivent être programmées dès maintenant

NOTRE SERVICE

- Inventorier la cryptographie employée sur votre SI
- Prioriser les actions à entreprendre immédiatement
- Remplacer la cryptographie obsolète
- Automatiser le renouvellement de vos certificats
- Éviter l'indisponibilité des services
- Gérer le risque Quantum

AVANTAGES

- Anticipation et tranquillité d'esprit sur ce nouvel enjeu
- Suivi du risque Quantum (HNDL)
- Assurance de l'utilisation d'algorithmes sûrs
- Assurance de la continuité des services employant des certificats renouvelés automatiquement
- Simplification la gestion du cycle de vie des certificats

PROCHAINE ÉTAPE

Contactez-nous pour une première évaluation.

Nous vous accompagnons pour/en vous :

1. Inventorier vos crypto-assets
2. Revoir vos politiques cryptographiques
3. Analyser votre exposition au risque HNDL
4. Planifier le projet PQC et prioriser les actions à entreprendre
5. Proposant une solution adaptée de gestion du cycle de vie des certificats

Nous vous aidons à transformer la cryptographie… d'un risque en un atout stratégique!

Prochaines étapes

- Planification d’un RDV (Diagnostic, Roadmap et Objectifs)
- 1 Organisation et lancement du projet selon les priorités établies
- Proposition d’une solution adaptée assurant la gestion de vos certificats
- Construction de votre trajectoire de transition vers le PQC

PRÊTS À DEVENIR CRYPTO AGILE ET PQC READY ? PARLONS-EN !

Votre interlocuteur chez SPIE ICS

« Assurer la souveraineté numérique, c'est faire de la cybersécurité une priorité : car maîtriser vos processus et vos données, c'est préserver votre autonomie tout en renforçant la résilience de votre organisation. »

spie.ch/gouverner

Frédéric Noyer

Head of Governance Services & Pentesting

Tél. +41 79 405 56 99

Mail frederic.noyer@spie.com