Orange Wholesale

Vers une cryptographie résistante aux attaques quantiques

FRnOG - 20 mars 2026

Orange Wholesale France est une entité de Orange Wholesale, une division du groupe Orange

Nos missions

Orange Wholesale apporte aux opérateurs et aux acteurs mondiaux du numérique des infrastructures résilientes et des solutions de connectivité dans le monde entier, entièrement sécurisées.

Nos clients peuvent intégrer facilement nos solutions à leurs réseaux, externaliser la complexité tout en gardant le contrôle et bénéficier de l'optimisation économique et environnementale de la mutualisation.

Ils font appel à Orange Wholesale pour :

- la qualité et la couverture de nos réseaux,

- l'expertise et l'engagement de nos équipes au service de nos clients

Nos services

Services de connectivité
Fixe, Mobile

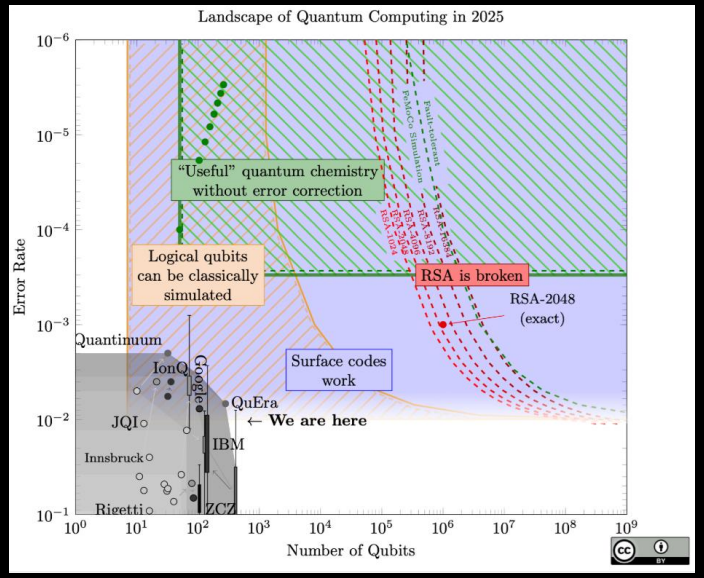
New : Fibre Dédiée, jusqu'à 400Gbp/s sur tout le territoire, 35M de prises disponibles.

Services d'Infrastructures
Backbone, Hébergement, Génie civil

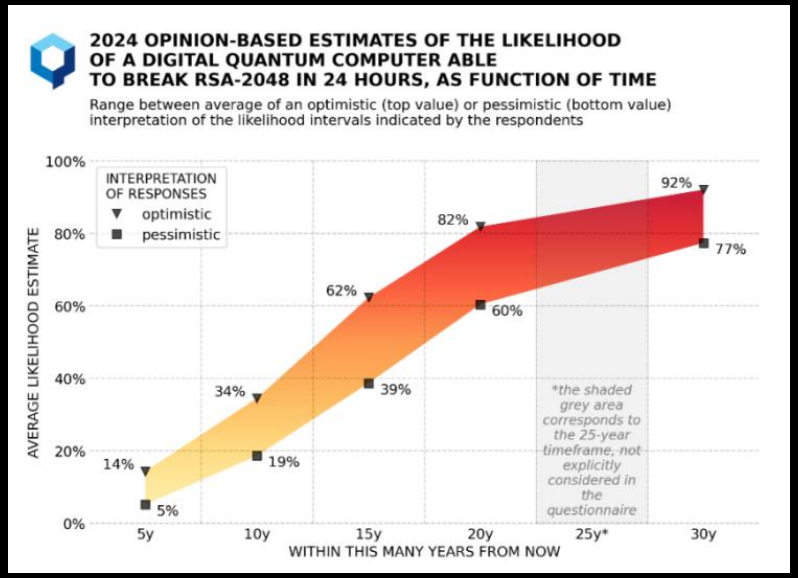
Services d'interconnexion
Déploiement et raccordement des infrastructures, des connexions et interconnexions.

La menace quantique

- La cryptographie moderne se fonde sur des problèmes mathématiques facilement calculables mais impossibles à inverser avec des ordinateurs classiques alors qu'un ordinateur quantique de capacité suffisante pourrait les calculer très rapidement.
- Les efforts de développement des ordinateurs quantiques s'accélèrent mais la date de disponibilité d'un « CRQC* » reste inconnue. Le BSI allemand l'estime pour 2040. Gartner Research le situe en 2034.



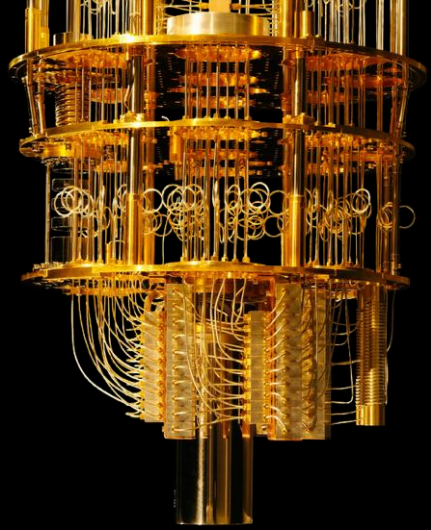
Source : Samuel Jacques, Université de Waterloo



Source : Global Risk Institute, Quantum Threat Timeline Report 2024

* Cryptographically Relevant Quantum Computer : ordinateur quantique suffisamment puissant pour exécuter les algorithmes capables de casser les standards de cryptographie actuels

La menace quantique



La cryptographie actuelle est vulnérable

- En premier lieu la cryptographie à clé publique (asymétrique) est complètement cassée par l'algorithme quantique de Shor
- Le chiffrement symétrique est aussi affecté mais de manière plus limitée par l'algorithme quantique de Grover (réduction quadratique*)

Une transition à engager dès maintenant

- Attaques rétroactives « Harvest now, decrypt later »
- Attaques en contrefaçon « Trust now, forge later »
- La transition post-quantique prendra du temps

$$T_{\text{DURÉE DE MIGRATION}} + T_{\text{DURÉE DE PROTECTION}} > T_{\text{MENACE QUANTIQUE}}$$

* Par exemple le niveau de sécurité de l'AES-128 serait réduit à un niveau équivalent à 64 bits

Les réponses à la menace quantique

Il existe 2 options très différentes face à la menace quantique :

PQC
« Cryptographie Post-Quantique »

Approche logicielle fournissant des algorithmes de cryptographie sécurisés contre la menace quantique

? Sécurité mathématique conjecturée
√ Authentification et chiffrement
√ Compatible avec les infrastructures existantes
√ Pas de limite de portée
X Interception difficile à détecter

QKD
« Distribution Quantique de Clés »

Approche matérielle utilisant les propriétés fondamentales de la physique quantique pour générer et distribuer des clés de cryptographie symétrique

√ Inviolabilité théorique
X Chiffrement uniquement
X Matériel spécialisé
X Portée limitée (80/100 km en fibre)
√ Interception détectable

La cryptographie à l'ère post-quantique (PQC)

A la suite d'une compétition internationale démarrée en 2016, le NIST [1] a officiellement publié en août 2024 3 algorithmes résistants à un ordinateur quantique.

- **ML-KEM / FIPS 203** **(dérivé de Crystals-Kyber) est un mécanisme d'encapsulation de clés**
- **ML-DSA / FIPS 204** **(dérivé de Crystals-Dilithium) génère des clés de signature électronique**
- **SLH-DSA / FIPS 205** **(dérivé de Sphincs+) permet de créer des clés publiques de plus petite taille que ML-DSA et sa sécurité est mieux établie mais au prix de signatures plus volumineuses et plus de temps de calcul.**

Un troisième algorithme de signature, NL-DSA (dérivé de Falcon) est en voie d'être standardisé par le NIST.

Algorithme	Catégorie de sécurité [2]	Taille des clés (octets)	
		Client Hello	Serveur Hello
X25519	X	32	32
ML-KEM-512	1	800	768
ML-KEM-768	3	1184	1088
ML-KEM-1024	5	1568	1568

Algorithme	Catégorie de sécurité [2]	Taille (octets)	
		Clé publique	Signature
Ed25519	X	32	64
RSA 2048	X	272	256
ML-DSA-44	1	1312	2420
ML-DSA-65	3	1952	3309
ML-DSA-87	5	2592	4627

Source : Post-Quantum signatures zoo de Thom Wiggers [3]

1 National Institute of Standards and Technologies : institut américain responsable de la définition des normes techniques aux Etats-Unis
2 Catégories de sécurité PQC standardisées par le NIST (cf.: https://postquantum.com/post-quantum/nist-pqc-security-categories/#mapping-pqc-categories-to-traditional-security-strengths)
3 https://pqshield.github.io/nist-sigs-zoo/

L’hybridation

Définition

Pour l’échange de clés ou la signature, l’hybridation consiste à combiner un algorithme de cryptographie post-quantique avec un algorithme de cryptographie classique (pré-quantique) connu de manière à ce que l’ensemble reste sûr même si un seul d’entre eux l’est.

Motivation

Les algorithmes PQC étant récents, leur sécurité intrinsèque et celle de leur implémentation n’est pas encore parfaitement établie.

La position des agences réglementaires

L’ANSSI considère que l’hybridation est impérative et ce au moins jusqu’en 2030 :
« *L'ANSSI insiste fortement sur le caractère essentiel de l'hybridation des algorithmes de cryptographie post-quantique partout où ils sont déployés, à la fois à court et moyen terme. Les seuls algorithmes post-quantiques pour lesquels l'ANSSI ne recommande pas un recours systématique à l'hybridation sont les algorithmes de signature fondés sur le hachage : SLH-DSA, XMSS et LMS.* **»** [2]

C’est aussi la position d’autres agences européennes (BSI allemand, NLNCSA en Hollande, Suède)

1 National Institute of Standards and Technologies : institut américain responsable de la définition des normes techniques aux Etats-Unis

2 ANSSI : FaQ sur la Cryptographie post-quantique (PQC) https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/faq-pqc/

Les algorithmes et protocoles à risque vis-à-vis d'un CRQC*

Algorithme / protocole	Niveau de risque	**Description du risque quantique**	**Recommandation**
RSA (1024-4096>)	Critique	Complètement cassé par l'algorithme de Shor	Migrer vers ML-KEM (pour l'encapsulation de clés) et ML-DSA (pour les signatures)
DH / ECDH	Critique	Complètement cassé	Migrer vers ML-KEM
ECDSA / ECC	Critique	Complètement cassé	Remplacer par ML-DSA
DSA	Critique	Complètement cassé	Remplacer par ML-DSA
SHA-1 / MD5	Elevé	Attaques par collisions (même avec un ordinateur classique)	Remplacer par SHA-256 ou plus
AES-128	Elevé	Réduction quadratique de la sécurité avec l'algorithme de Grover	Mettre à jour en AES-256
Protocole TLS 1.2		Ne permet pas les protocoles d'échange de clés post-quantiques	Remplacer par TLS 1..3

* Cryptographically Relevant Quantum Computer: Ordinateur quantique suffisamment puissant pour exécuter les algorithmes capables de casser les standards de cryptographie actuelle

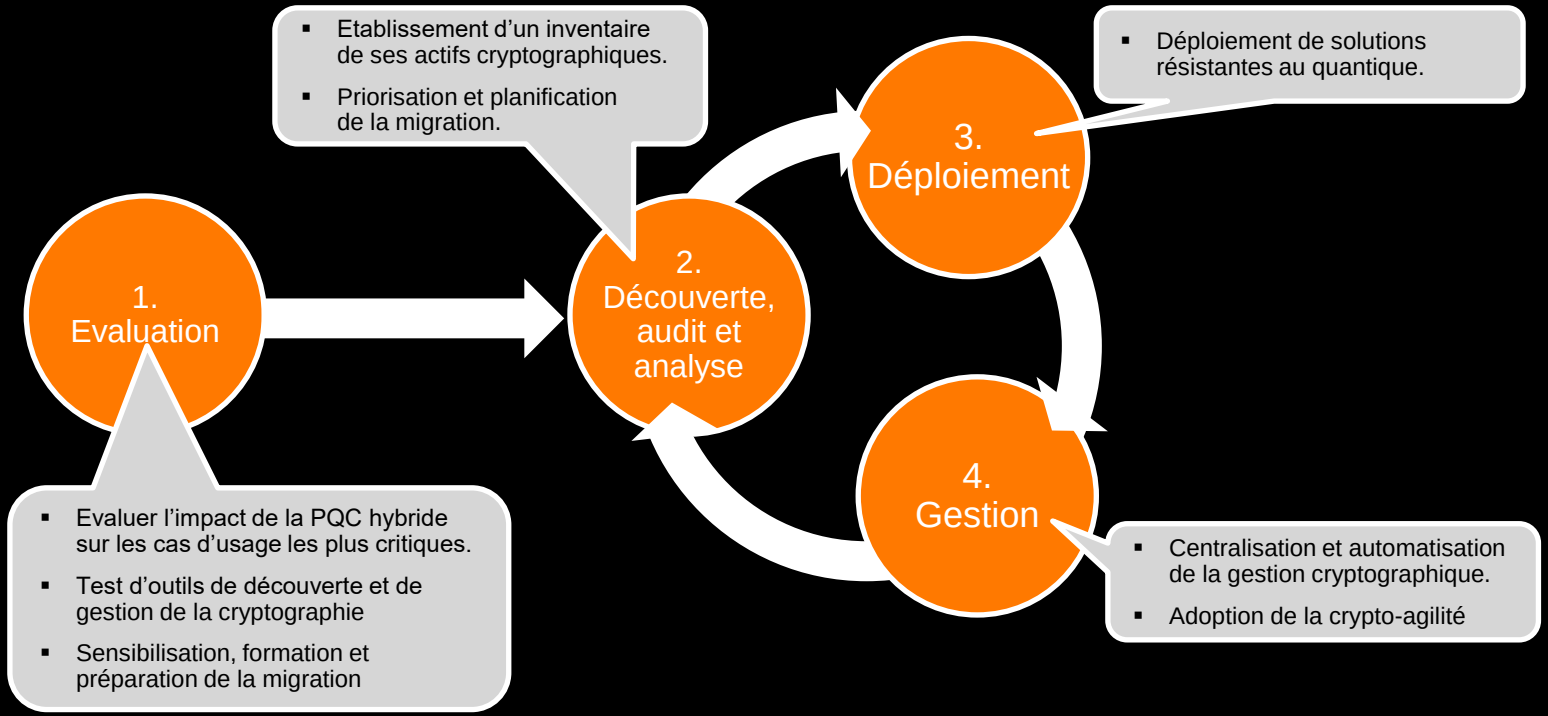
Les algorithmes à privilégier

Algorithmes dont la catégorie de sécurité NIST est au moins égale à 3 (sécurité considérée comme au moins équivalente à celle de l'AES-192). L'ANSSI recommande d'utiliser de préférence le niveau le plus élevé possible.

Fonction	Algorithmes	Catégorie de sécurité	**Notes**
Signature	ML-DSA-65 ML-DSA-87	3 5	Algorithme post-quantique standardisé par le NIST en 2024 (FIPS 204 ex. Crystals-Dilithium) basé sur les réseaux euclidiens
Signature	SHL-DSA-SHA2-192 SHL-DSA-SHAKE2-192 SHL-DSA-SHA2-256 SHL-DSA-SHAKE2-256	3 3 5 5	Basé sur des fonctions de hachage, sa sécurité est mieux établie mais au prix de signatures plus volumineuses et plus de temps de calcul.
Chiffrement symétrique	AES-192 AES-256	3 5	Considérés comme sûrs
Hachage	SHA-384, SHA3-384 SHA-512, SHA3-512	4 5	Considérés comme sûrs
Signature de firmware/logiciel	LMS, XMSS	3 ou 5	Ces schémas de signature maintiennent un état interne (stateful) et ne sont adaptés que dans les contextes où très peu de signatures sont réalisées
Echange de clés dans TLS 1.3	SecP256r1MLKEM768 X25519MLKEM768 SecP384r1MLKEM1024	3 3 5	Pour tenir compte des recommandations de l'ANSSI, seuls les algorithmes hybrides sont évoqués. Les algorithmes de catégorie de sécurité < 3 (comme ML-KEM-512) ou ceux ayant précédés la standardisation ne sont pas retenus.

La crypto-agilité, une transformation de long terme

Aujourd'hui la cryptographie n'est pas gérée activement. **La crypto-agilité est un processus permettant d'adapter rapidement un système aux évolutions des algorithmes cryptographiques, aux nouvelles menaces et aux standards émergents.**



La PQC à Orange International Network Infrastructure Services

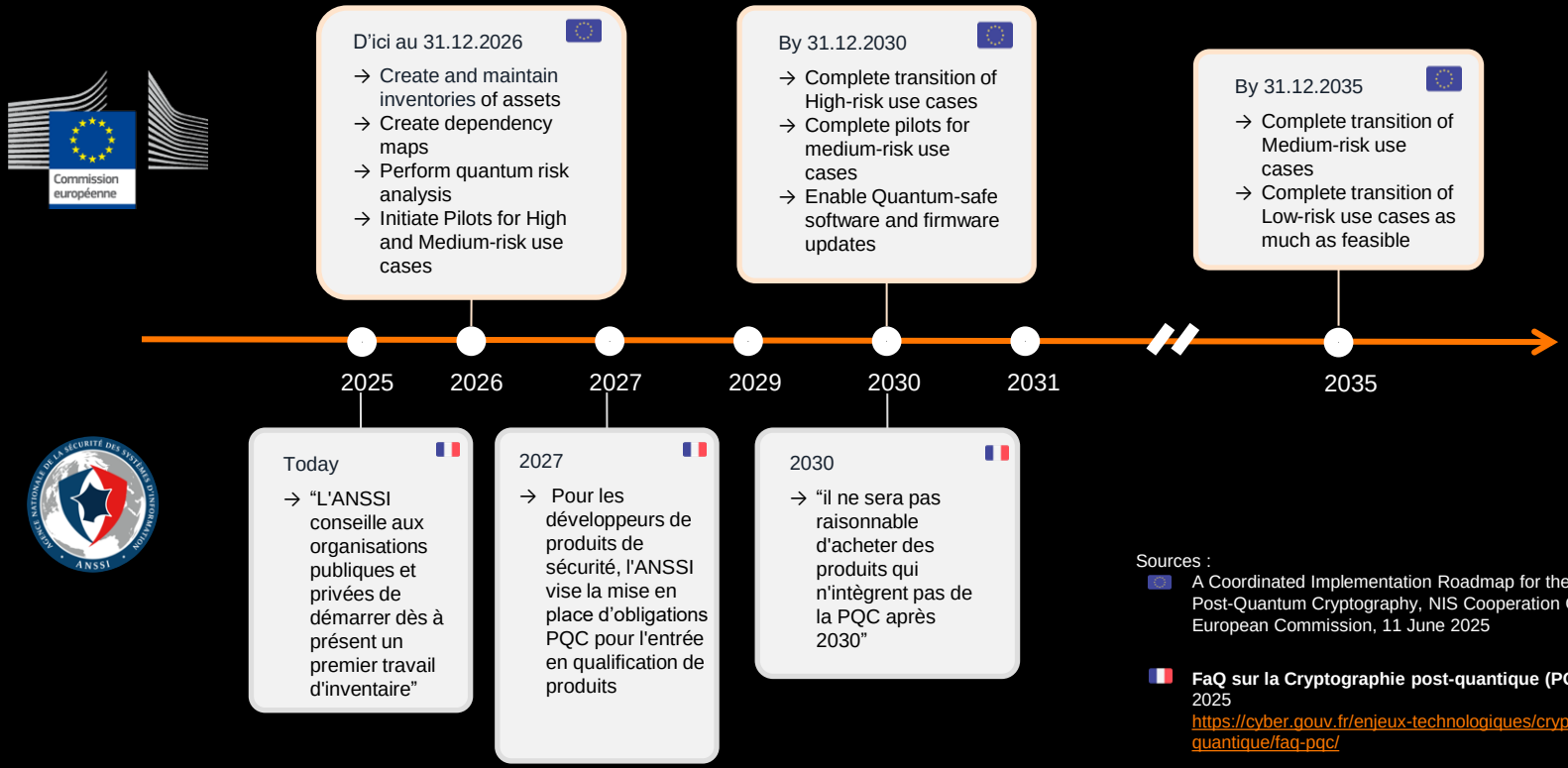
Nos axes de travail

- Priorité aux réseaux d'administration (control plane)
- Test de solutions de découverte et d'analyse cryptographique engagé en partenariat avec Orange Innovation
- Définition d'une configuration résistante au quantique de nos tunnels IPSEC
- Pour les équipements qui ne peuvent pas évoluer, encapsulation de leur trafic dans des tunnels IPSec résistants au quantique
- Configuration des VPN WireGuard résistants au quantique
- Etude d'opportunité d'un chiffrement résistant au quantique au niveau de nos backbones

Le volet concernant l'authentification post-quantique n'est pour l'instant pas engagé car il est dépendant de la PKI du Groupe Orange dont l'évolution post-quantique n'est pas encore planifiée.

Merci

La feuille de route en France et en Europe

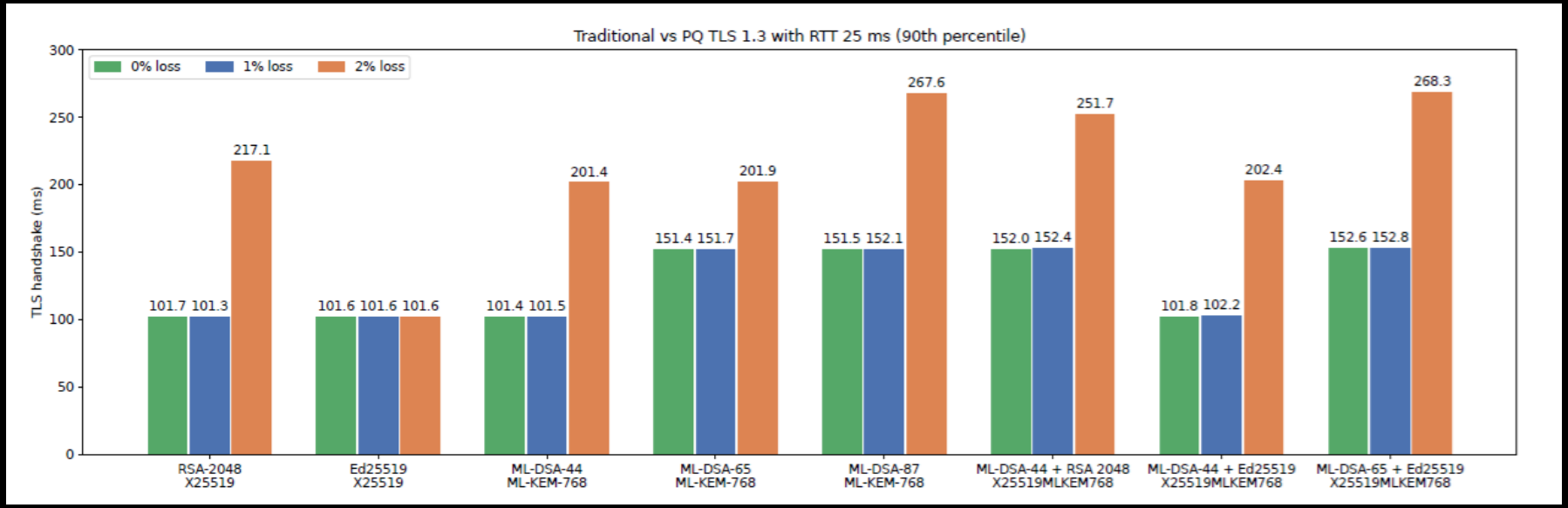


Sources :

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, NIS Cooperation Group, European Commission, 11 June 2025

FaQ sur la Cryptographie post-quantique (PQC), octobre 2025
https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/faq-pqc/

Impact de la PQC sur les délais d'établissement TLS



Source : Iyán Méndez Veiga, Lucerne University of Applied Sciences and Arts. Benchmarking TLS 1.3 with PQC under Realistic Network Conditions
http://dx.doi.org/10.5281/zenodo.17799886

Quelques références

1. ANSSI. Posture générale et actions de l'ANSSI sur la PQC. 2025.
   https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/
2. Commission européenne. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. 2025.
   https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
3. ANSSI. Avis de l'ANSSI sur la migration vers la cryptographie post-quantique. 2024.
   https://messervices.cyber.gouv.fr/guides/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0
4. NIST. Transition to Post-Quantum Cryptography Standards. 2024.
   https://csrc.nist.gov/pubs/ir/8547/ipd
5. A joint statement from partners from 18 EU member states. 2024.
   https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html
6. Cloudflare Radar.
   https://radar.cloudflare.com/post-quantum
7. ANSSI – Transition Post-Quantique de TLS 1.3
   https://messervices.cyber.gouv.fr/guides/Transition-post-quantique-protocole-TLS-1-3
8. ANSSI. Transition Post-Quantique d'Ipsec. 2026.
   https://messervices.cyber.gouv.fr/guides/Transition-post-quantique-protocole-IPsec
9. ANSSI – Transition Post-Quantique de SSHv2
   https://messervices.cyber.gouv.fr/guides/Transition-post-quantique-protocole-SSHv2