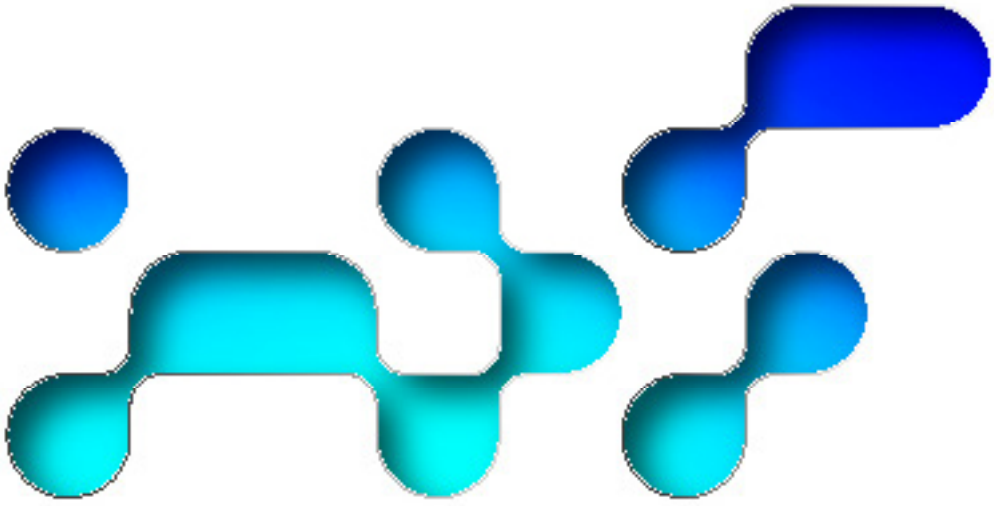
CAMPUS CYBER

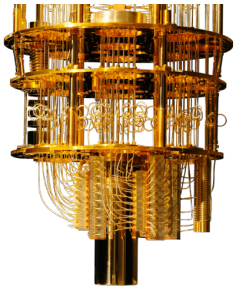
MENACE QUANTIQUE & CRYPTOGRAPHIE POST-QUANTIQUE

COMPRENDRE CET ENJEU MAJEUR DE SÉCURITÉ,
POURQUOI IL FAUT AGIR MAINTENANT



GT : CRYPTOGRAPHIE POST-QUANTIQUE

LA MENACE QUANTIQUE UN ENJEU SYSTEMIQUE DE SECURITE



Un **ordinateur quantique efficace** est une machine capable de casser les algorithmes de cryptographie à clé publique (dits asymétriques) les plus couramment utilisés. Un tel ordinateur **remettra en cause les fondements** sur lesquels repose la **sécurité** d'Internet et de nos infrastructures IT/OT.

Or, en pratique, les algorithmes à clé publique sont présents dans de nombreux systèmes.

Cela signifie que la **sécurité** de la plupart des **services et infrastructures numériques** que nous utilisons est menacée d'être **réduite à néant.**

Internet sécurisé | VPN | Apps | Blockchain | Identités | IoT | Signature | Paiements

Toutes les organisations publiques et privées sont concernées et vont avoir à conduire de vastes plans de transformation et de migration de leurs infrastructures IT/OT vers des solutions résistantes aux attaques quantiques.

Les algorithmes **symétriques** sont souvent utilisés en **combinaison** avec des algorithmes **asymétriques** (pour l'échange authentifié des clés secrètes).

Déployer des algorithmes symétriques **quantiquement sûrs** ne fait sens que si les algorithmes asymétriques utilisés au préalable sont eux-mêmes résistants aux attaques quantiques.

CRYPTOGRAPHIE ASYMÉTRIQUE (CLÉ PUBLIQUE) ET ALGORITHMES MENACÉS

Tous les **algorithmes à clé publique les plus utilisés** (basés sur deux grands problèmes mathématiques : logarithme discret et factorisation) sont **vulnérables** face à un ordinateur quantique.

FONCTION	PROPRIETE	ALGORITHMES	
Chiffrement	Confidentialité	RSA,	ElGamal
Signature	Authentification	RSA,	ECDSA
Echange de clé	Partage de secret	RSA,	ECDH

Sécurité basée sur le problème { factorisation | log. discret

Problèmes mathématiques **solubles** avec l'**algorithme quantique de Shor**

LA CRYPTOGRAPHIE SYMÉTRIQUE (CLÉ SECRÈTE) PAS MENACÉE DE MANIÈRE STRUCTURELLE

Les **algorithmes symétriques** (ou à clé secrète) sont **moins impactés** par les attaques quantiques (algorithme de Grover et ses variantes). Si le coût réel de l'algorithme de Grover est matière à discussion, l'option la plus raisonnable pour s'en prémunir consiste à **doubler la taille des clés.**

FONCTION	PRE-QUANTIQUE	POST-QUANTIQUE
Chiffrement	AES 128	AES 256
Hachage	SHA-256	SHA-384, SHA-512

LA MENACE QUANTIQUE POURQUOI FAUT-IL AGIR DES AUJOURD'HUI ?

Au-delà des estimations des experts sur la date d'arrivée d'un ordinateur quantique suffisamment puissant (CRQC, Cryptographically Relevant Quantum Computer), 2030, 2035, 2040 ou plus – le **risque** et son **impact** sont considérés par les agences de sécurité comme **élevés** et certaines données sont déjà concernées par la menace. Il faut donc agir dès aujourd'hui et **se préparer à la transition.**

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 »

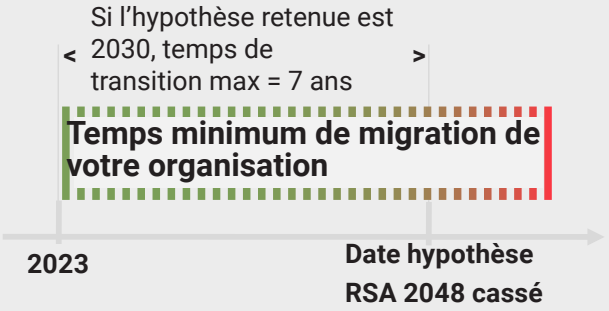
« HARVEST NOW, DECRYPT LATER » – LES DONNÉES SENSIBLES À LONGUE DURÉE DE VIE DÉJÀ EN RISQUE

Certaines organisations sont en capacité de **collecter** massivement nos communications et données pour les stocker, en vue de les **décrypter** quand un ordinateur quantique suffisamment puissant sera disponible. Les **données secrètes à longue durée** de vie sont dès aujourd'hui concernées.

« L'ANSSI recommande d'appliquer une défense en profondeur post-quantique dès que possible pour les produits de sécurité visant à offrir une protection longue durée des informations (jusqu'après 2030) » (avril 2022)

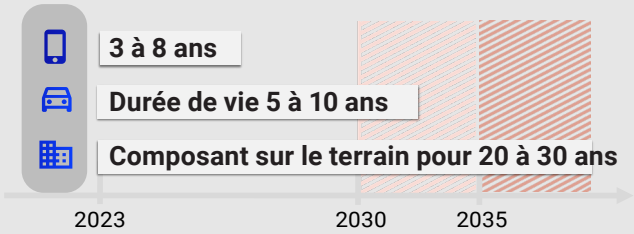
LE TEMPS DE MIGRATION VERS DES INFRASTRUCTURES RÉSISTANTES AU QUANTIQUE DOIT ÊTRE ANTICIPÉ

Il est nécessaire d'être prêt le jour où un ordinateur quantique suffisamment puissant existera. La **migration** d'une grande entreprise vers le post-quantique prendra **plusieurs années** (5, 10 ans…). Il est nécessaire de **se prépare**r et **d'anticiper** ce temps de transition.



LE CYCLE DE VIE DES SYSTÈMES ET PRODUITS IT EST UN FACTEUR À PRENDRE EN COMPTE

Certains systèmes informatiques ou produits embarqués sont déployés sur le terrain pour des **périodes longues**, parfois 20 à 30 ans dans le cas de **l'IoT** industriel, **sans capacité de mettre à jour** la cryptographie sous-jacente si ceci n'a pas été anticipé.



LA SOLUTION LA CRYPTOGRAPHIE POST-QUANTIQUE

PRINCIPE DE LA CRYPTOGRAPHIE POST-QUANTIQUE (PQC)

Les **algorithmes à clé publique les plus déployés** reposent sur des problèmes mathématiques (logarithme discret, factorisation) qui peuvent être résolus avec **l'algorithme quantique de Shor.**

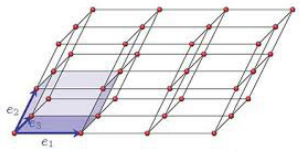
Ces algorithmes utilisés actuellement ne garantissent donc aucune sécurité face à un ordinateur quantique.

L'algorithme de Shor est si efficace que l'augmentation de la taille des clés asymétriques ne constitue pas une solution. Pour être résistant à cette attaque, il faudrait par exemple utiliser des clés RSA de 1 téra-octet (au lieu de 384 octets actuellement) ce qui est totalement impraticable.

La **remédiation** consiste à utiliser des algorithmes à clé publique basés sur des **problèmes mathématiques** différents, non solubles en pratique avec un ordinateur quantique : ce sont les **algorithmes post-quantiques ou résistants aux attaques quantiques.**

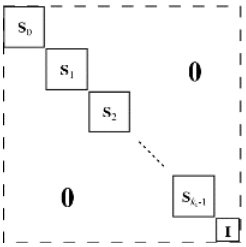
Les algorithmes à clé publique post-quantiques fournissent des **fonctionnalités similaires** aux algorithmes classiques et sont destinés à être **déployés sur les infrastructures informatiques actuelles** en réponse à cette menace créée par l'ordinateur quantique.

ILLUSTRATION DES PROBLÈMES MATHÉMATIQUES SOUS-JACENTS

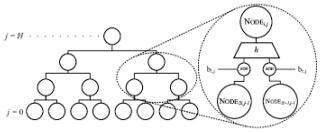


Réseaux euclidiens (favoris)

Isogénies (outsider)



Codes correcteurs (choix conservateur)



Fonctions symétriques (choix conservateur)

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

$$\vdots$$

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

Equations multivariées (outsider)

HYBRIDATION : CLASSIQUE + POST-QUANTIQUE

L'**hybridation** vise à **combiner** dans les protocoles les algorithmes de cryptographie **pré-quantiques** avec les algorithmes **post-quantiques** afin de garantir un niveau de sécurité au moins **égal à l'existant** tout en se préparant à la **menace future.**

Algorithmes classiques
Confiance établie
Vulnérables au quantique
RSA, ECC
Solutions existantes (ex : CNSA)

Algorithmes post-quantiques
Maturité moindre
Resistants au quantique
PQC
Nouvelles recommandations (NIST, ANSSI...)

Algorithmes hybrides
Sécurité : meilleure des deux
Performances : plus de compléxité

PROTOCOLES DE COMMUNICATION

https:// → TLS hybride post-quantique

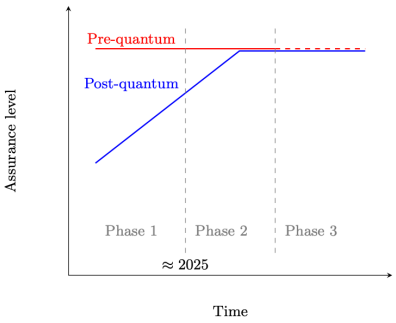
Les algorithmes post-quantiques doivent être implémentés dans les protocoles de communication normalisés et les mécanismes cryptographiques communément utilisés.

Cela **impacte nos usages quotidiens** : aller sur un site web sécurisé, envoyer un email, faire un paiement par carte bancaire, signer un document, authentifier une identité...

Le **déploiement des algorithmes post-quantiques** implique un minimum d'**adaptation** (algorithmes de chiffrement, signature). Dans certains cas, un **remplacement direct** d'algorithme n'est **pas possible** (échange de clé Diffie-Hellman) et une **refonte importante des protocoles** est nécessaire.

LES AGENCES NATIONALES STIMULENT LA TRANSITION

Les agences de sécurité nationales se positionnent et fournissent progressivement leurs préconisations de méthode et de calendrier.



- Il faut s'appuyer sur les processus en cours de sélection de **nouveaux algorithmes**, largement **étudiés** par la communauté scientifique.
- **L'ANSSI** en France ou le BSI en Allemagne soutiennent la démarche du NIST aux Etats-Unis, mais font aussi **leurs propres recommandations** comme pour l'usage de l'algorithme FrodoKEM.
- La mise en place de **protocoles hybrides** est le **seul mode recommandé** (en Europe) de mise en place de la cryptographie à clé publique post-quantique.
  A partir de 2024-**2025**, des **visas de sécurité post-quantique** pourront être délivrés.
- A partir de cette même date, ce mode de cryptographie hybride pourra être rendu **obligatoire** dans certains contextes.

PROCESSUS DE NORMALISATION DU NIST US

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

L'administration américaine du NIST (National Institute of Standard and Technology) a lancé dès 2016 un vaste processus pour faire appel à la communauté cryptographique mondiale et **sélectionner de nouveaux algorithmes** comme normes de cryptographie post-quantique.

Tour 1 – 82 propositions – 2016

Tour 2 – 26

Tour 3 - 7

Premières sélections en juillet 2022

CRYSTALS-KYBER /
CRYSTALS-DILITHIUM / FALCON / SPHINCS+

D'autres pays, comme la Chine ou la Corée du Sud, ont organisé leurs propres processus et choix d'algorithmes post-quantiques.

LES ETATS-UNIS EN ACTION POUR RÉPONDRE À LA MENACE ET METTRE EN PLACE UN ÉCOSYSTÈME AVANCÉ

- **NIST** (juillet 2022) : **première sélection d'algorithmes post-quantiques.**
- **NCCoE** (juillet 2022) : lancement de l'initiative **« Migration to PQC »** avec 20 industriels.
- **NSA** (septembre 2022) : mise à jour du **référentiel de cryptographie pour les Systèmes Nationaux** de Sécurité.
- **Maison Blanche** (novembre 2022) : publication du mémorandum NSM-10 (et vote d'une loi au Congrès), demandant aux agences fédérales de **lancer la transition : inventaire, définition de plans de transition**, conduite de pilote en production avant la finalisation des normes, mise en place d'une gouvernance et d'un reporting centralisé, avec premier jalon en mai 2023.
- **Homeland Security Department** (octobre 2022) : annonce d'un objectif de migration d'ici 2030.
- **Nouvelle Stratégie Nationale de Cybersécurité** (mars 2023) : la Cryptographie Post-Quantique est un pilier.

Au coeur de nombreux enjeux industriels, les organismes de normalisation transverses (IETF, ETSI, ITU, ISO/IEC, IEEE…) ou métier (GSMA, EMVCo…) ont des groupes de travail actifs pour la définition de normes actualisées.

LES ACTIONS A MENER

La **migration** vers des infrastructures résistantes au quantique dans un **écosystème fortement connecté** et **interopérable** représente un **défi de transformation inédit.**

En pratique, chaque organisation doit **intégrer la menace quantique** dans sa cartographie des risques majeurs et doit s'engager sur le chemin de la **transition** avec une vision globale de moyen terme à 5 ou 10 ans et des actions qui peuvent être déclenchées dès aujourd'hui.

DES ACTIONS-CLÉS

- **Inventaire cryptographique** pour cartographier la cryptographie sous-jacente.
- **Pilotes** pour tester des solutions techniques sur des cas d'usage, comprendre les enjeux de migration et construire une stratégie cohérente et globale de transition.
- **Crypto-agilité** : comprendre les enjeux de crypto-agilité à différents niveaux (algorithmes, protocoles, systèmes, cas d'usage de bout en bout) et intégrer la crypto-agilité pour préparer l'arrivée de la cryptographie hybride post-quantique.
- **Politique d'achat** : intégrer la dimension post-quantique dans les cahiers des charges des solutions informatiques (HSM, PKI, applications de communication, logiciels métiers, IoT et systèmes embarqué, etc.)

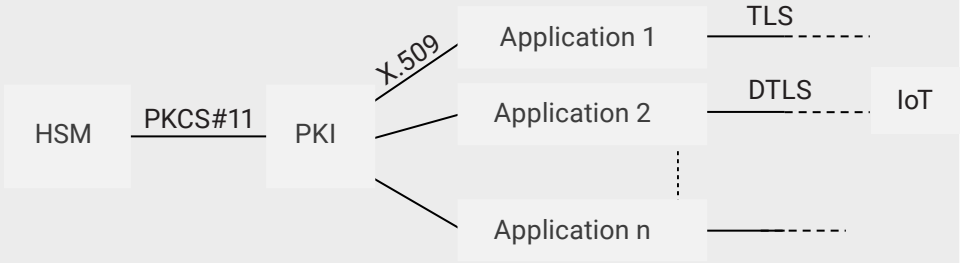
UNE VISION GLOBALE : LE PLAN DE TRANSITION POST-QUANTIQUE

Toutes les organisations privées ou publiques ont à :

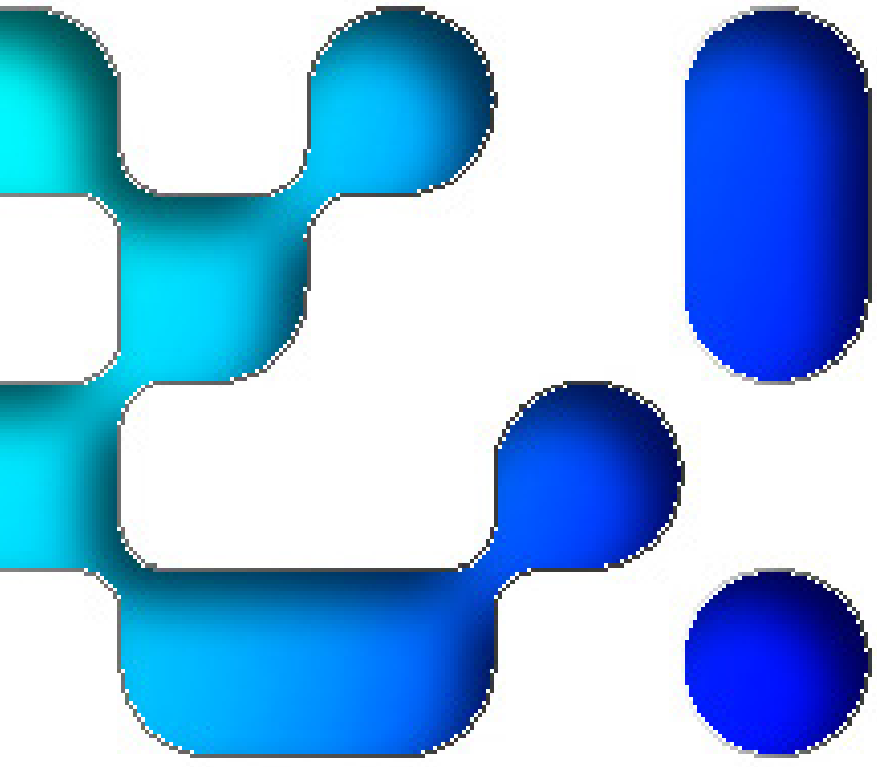
1. **définir des plans de transition** vers le post-quantique incluant **l'inventaire** de leur **cryptographie**, la cartographie des **données critiques** et la **priorisation** ;
2. **opérer la migration** vers des infrastructures ou produits embarqués résistants au quantique ;
3. **mettre en place** une organisation et des **solutions crypto-agiles** pour la conduite des opérations et faciliter **l'application des recommandations** les plus récentes.

DES DÉFIS CONCRETS DE MIGRATION DANS UN ENVIRONNEMENT INTEROPÉRABLE

Au-delà de la mise à jour de solutions matérielles ou logicielles indépendantes, il s'agit d'assurer **la cohérence, l'interconnexion, l'interopérabilité de bout en bout.**



Un document collaboratif produit par le GT PQC - Sensibilisation dont les entités suivantes sont membres :



CAMPUS CYBER
5 - 7 RUE BELLINI
92800
PUTEAUX

https://campuscyber.fr/