Transition post-quantique : aspects techniques

Jérôme Plût—jerome.plut@ssi.gouv.fr

Laboratoire de Cryptographie, ANSSI

2024-06-25 PTCC

1. Menace quantique et sécurité post-quantique

Que peut faire un ordinateur quantique ?

- **Algorithme de Shor :** un ordinateur quantique suffisamment grand peut résoudre les problèmes du *logarithme discret* et de la *factorisation* en *temps polynomial* (c.à.d. très efficacement).
  - Ceci casse : RSA, (EC)DSA, (EC)DH...
  - (soit à peu près toute la cryptographie asymétrique actuellement utilisée !)
  - Ordre de grandeur : possiblement quelques minutes.

- **Algorithme de Grover :** un ordinateur quantique *extrêmement* grand pourrait résoudre le problème de la *recherche exhaustive* en temps *exponentiel* $2^{n/2}$ (c.à.d. un peu efficacement).
  - Il s'agit donc d'une attaque générique, valable contre tout algorithme cryptographique imaginable.
  - En particulier, *toute la cryptographie symétrique* est affectée.
  - Mais cette attaque reste inefficace (et non parallélisable).

- Quelques **cas particuliers supplémentaires**: possiblement une recherche de collision en racine cubique...

Évaluation de la menace quantique

L'ordinateur quantique utile cryptographiquement n'existe pas...

Évaluation de la menace quantique

L'ordinateur quantique utile cryptographiquement n'existe **probablement** pas **maintenant**...

- Prédictions (Mosca) : « 1 chance sur 7 en 2026 ».
  - (non falsifiable donc non scientifique !)
  - ... mais les analyses de sécurité considèrent les événements de probabilité $> 2^{-128}$.

Évaluation de la menace quantique

L'ordinateur quantique utile cryptographiquement n'existe **probablement** pas **maintenant**...

- Prédictions (Mosca) : « 1 chance sur 7 en 2026 ».
  - (non falsifiable donc non scientifique !)
  - ... mais les analyses de sécurité considèrent les événements de probabilité $> 2^{-128}$.

MAIS

- Le déploiement de la cryptographie résistante *pourrait* prendre plus longtemps que la concrétisation de la menace quantique.
  - Théorème de Mosca: *"if $x + y > z$ then worry."*
- La menace existe déjà : **attaques rétroactives.**

Attaques rétroactives

- Contre la *confidentialité* en général : « récolter maintenant, décrypter plus tard »;
  - ☞ Affecte le chiffrement asymétrique (courriels chiffrés)...
  - ☞ mais également l'échange de clés (TLS).

- Contre l'*authenticité* dans certains cas : (« vérifier maintenant, contrefaire plus tard » ?)
  - ☞ possibilité de contrefaire des mises à jour logicielles dans le futur;
  - ☞ documents authentifiés de longue durée de vie (identité, contrats...);
  - ☞ les échanges de clé authentifiés ne sont **pas** affectés maintenant, (mais devront tout de même être mis à jour avant l'arrivée de l'ordinateur quantique).

Le futur de la cryptographie asymétrique ?

Cryptographie quantique

Position extrême : *Abandonner la cryptographie* et s'appuyer sur la sécurité physique.

- Remplace *certaines fonctionnalités* de la cryptographie classique.
  - Échange de secret résistant à toute attaque algorithmique.
  - Les participant doivent être *authentifiés (classiquement)*.
  - Équivalent au masque jetable (ne remplace que *certaines* fonctionnalités de la cryptographie standard).
- La sécurité physique est encore un sujet de recherche ouvert :
  - Hypothèses fortes sur les sources (ex. : source de photons uniques), le canal et les récepteurs (ex. : mode Geiger).
  - Intrinsèquement fragile face aux attaques en déni.
- À l'état de **science-fiction** pour l'instant.
- Position commune avec d'autres agences européennes :
  - https://cyber.gouv.fr/en/actualites/uses-and-limits-quantum-key-distribution
  - https://cyber.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications

Position extrême : *Abandonner la cryptographie* et s'appuyer sur la sécurité physique.

- Remplace *certaines fonctionnalités* de la cryptographie classique.
  - Échange de secret résistant à toute attaque algorithmique.
  - Les participant doivent être *authentifiés (classiquement)*.
  - Équivalent au masque jetable (ne remplace que *certaines* fonctionnalités de la cryptographie standard).
- La sécurité physique est encore un sujet de recherche ouvert :
  - Hypothèses fortes sur les sources (ex. : source de photons uniques), le canal et les récepteurs (ex. : mode Geiger).
  - Intrinsèquement fragile face aux attaques en déni.
- À l'état de **science-fiction** pour l'instant.
- Position commune avec d'autres agences européennes :
  - https://cyber.gouv.fr/en/actualites/uses-and-limits-quantum-key-distribution
  - https://cyber.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications

Cryptographie résistante à l'ordinateur quantique

- La cryptographie *symétrique* n'est que faiblement affectée par le calcul quantique (algorithme de Grover).
  - Précaution suffisante : doubler toutes les tailles de clés symétriques.
- Toute la cryptographie asymétrique utilisée (pré-2020) est irrémédiablement vulnérable à l'algorithmique quantique.
  - Solution : remplacer le logarithme discret (et la factorisation)...
  - ... par d'*autres problèmes mathématiques*.

Cryptographie post-quantique

(c'est en fait un sous-ensemble de la cryptographie classique !).

- Remplacer les problèmes mathématiques vulnérables par de nouvelles familles de problèmes.
  - Les problèmes accessibles au calcul quantique sont les plus *structurés* : groupes (abéliens), fonctions périodiques...

2. La transition post-quantique

Référentiel des mécanismes cryptographiques

- Pas de « liste blanche » d'algorithmes approuvés.
  - Ne pas fermer la porte à l'utilisation d'algorithmes ayant des cas d'usage spécifiques ou innovants.
- Une liste de critères par famille d'algorithmes.
  - ☞ pour les chiffrement par bloc : taille de clé et de bloc ;
  - ☞ pour le logarithme discret : taille du module, processus de génération,
- Pour les algorithmes ne rentrant pas dans ces familles, une *analyse ad-hoc* est nécessaire
  - ☞ (en s'appuyant au besoin sur les résultats académiques).
  - ☞ Un chiffrement par bloc exotique respectant les conditions de taille de clé et de bloc ne *sera pas* automatiquement approuvé !
- Les règles ne portent pas que sur des algorithmes individuels mais également sur la manière de les combiner.

Cryptographie résistante au calcul quantique

Doctrine ANSSI

- https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique
- https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0

- Remplacer tous les algorithmes pré-quantiques par des algorithmes *post-quantiques* « équivalents »
- ...**sans perte de sécurité** durant la transition.

La cryptographie post-quantique est-elle assez mûre ?

- Les algorithmes sont-ils sûrs ?
- Les protocoles sont-ils prêts ?
- Les implémentations sont-elles robustes ?

Hybridation

Hybridation

- Combiner un schéma pré-quantique *reconnu* avec un schéma *post-quantique* plus risqué...
- ... en garantissant une sécurité aussi forte que *la plus robuste* des deux primitives.
  - c'est-à-dire : il existe une preuve mathématique que casser la combinaison nécessite de casser **les deux** primitives.

La combinaison ajoute une protection contre la menace quantique tout en garantissant la non-régression.

☞ Méthodes d'hybridation : à la fin de cet exposé.

- **Coût :** la somme des parties classique et post-quantique.
  - La partie classique est généralement plus légère que la partie post-quantique (en bande passante).
- L'hybridation classique + clé (symétrique) pré-partagée est acceptée.
  - Ne garantit pas la PFS post-quantique.

Crypto-agilité

Crypto-agilité

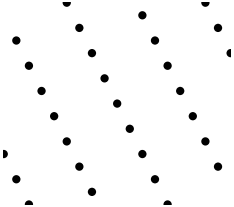
Un système est *crypto-agile* s'il est possible de mettre à jour ses algorithmes cryptographiques.

- Ceci permet de construire dès maintenant des systèmes qui pourront être mis à jour avec des algorithmes post-quantiques stabilisés.
- Contrainte : dimensionnement suffisant du système.

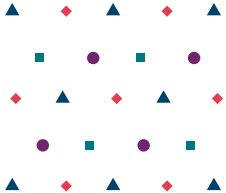
Familles d'algorithmes post-quantiques

Familles d'algorithmes post-quantiques

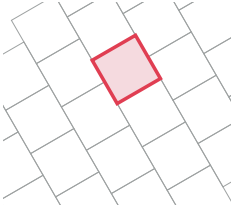
Réseaux euclidiens



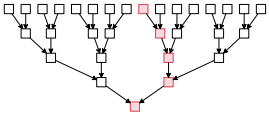
(Réseaux structurés)



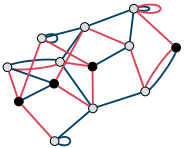
Codes correcteurs



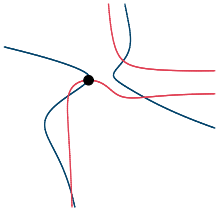
Fonctions de hachage



Graphes d'isogénies



Équations multivariées



Familles d'algorithmes post-quantiques

Réseaux euclidiens

- largement étudiés depuis 2005;
- nombreux usages (encapsulation de clé, signature, chiffrement homomorphe)...

(Réseaux structurés)

- cas particulier des réseaux;
- plus efficace mais hypothèse de sécurité plus forte.

Codes correcteurs

- certaines caractéristiques communes avec les réseaux ;
- étudiés depuis les années 1970;
- intérêt accru comme schémas post-quantiques.

Fonctions de hachage

- peu efficaces;
- hypothèse de sécurité minimale ;
- (seront discutées spécifiquement)

Graphes d'isogénies

- nombre restreint de cas d'usage ;
- compréhension mathématique probablement incomplète, plusieurs schémas ont été attaqués;
- possibles solutions de repli ou adaptées à des cas spécifiques.

Équations multivariées

Signatures basées sur le hachage

- Ces primitives ne reposent pas sur des problèmes mathématiques, mais uniquement sur des *fonctions de hachage*.
  - Elles disposent de preuves mathématiques ramenant leur sécurité à celle de certains problèmes : préimage sous contrainte, etc.
  - sécurité $\approx n$ bits (classique), $\approx n/2$ bits (quantique).
- Leur sécurité est donc **déjà reconnue**.
- Les signatures sont **très longues**.

Signatures à état

- **Nombre limité de signatures par clé** mais signatures plus compactes.
- À la clé privée est associée un *compteur* qui doit être incrémenté à chaque signature.
- La réutilisation du compteur *compromet immédiatement* la sécurité.
- Impossibilité de dupliquer une clé de signature.

Processus de standardisation post-quantique du NIST

- Processus démarré en 2016.
- A permis de condenser l'attention de la communauté scientifique sur un nombre restreint de primitives.
- Après trois tours de sélection, les algorithmes suivants sont retenus (depuis 2022) et en cours de standardisation :

	Encapsulation de clé	Signature
Réseaux (structurés)	ML-KEM (Kyber)	ML-DSA (Dilithium) FN-DSA (Falcon)
Hachage		SPHINCS+

- En outre, un quatrième round est en cours entre trois mécanismes d'encapsulation basés sur les codes :
  BIKE, Classic McEliece et HQC.
- Une compétition supplémentaire est ouverte pour les signatures (non basées sur les réseaux structurés).

Maturité de la cryptographie post-quantique

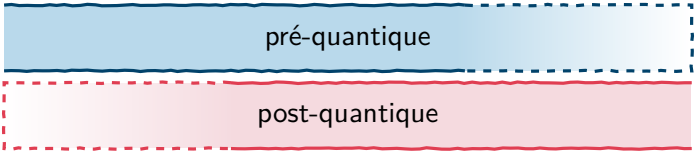
Le niveau de maturité de la cryptographie post-quantique ne doit pas être sur-estimé.

- Il est (grossièrement) comparable à celui de RSA dans les années 1990.
- Sécurité des algorithmes :
  - Compréhension de la difficulté (classique ou quantique) des problèmes mathématiques sous-jacents ;
  - Dimensionnement et choix de la famille d'algorithme...
- Sécurité des *implémentations* :
  - attaques par canaux auxiliaires,
  - intégration dans les protocoles...

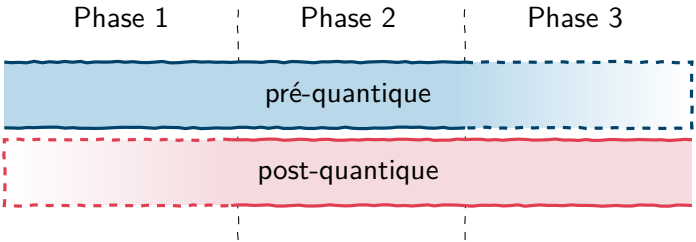
La publication (imminente) des standards NIST n'entraînera pas la maturité immédiate de la cryptographie post-quantique.

La cryptographie post-quantique doit être déployée aussi rapidement que possible, y compris avant la complète maturité des algorithmes et de leurs implémentations.

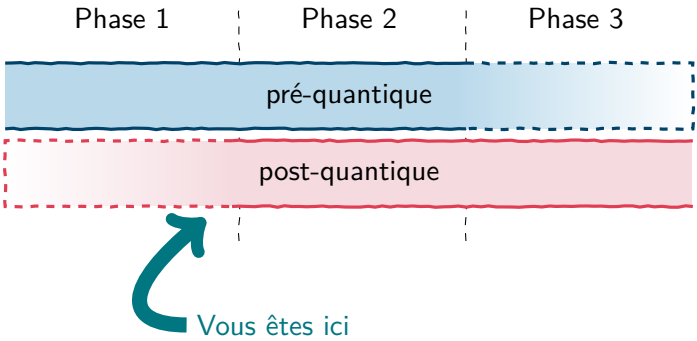
Transition en trois phases



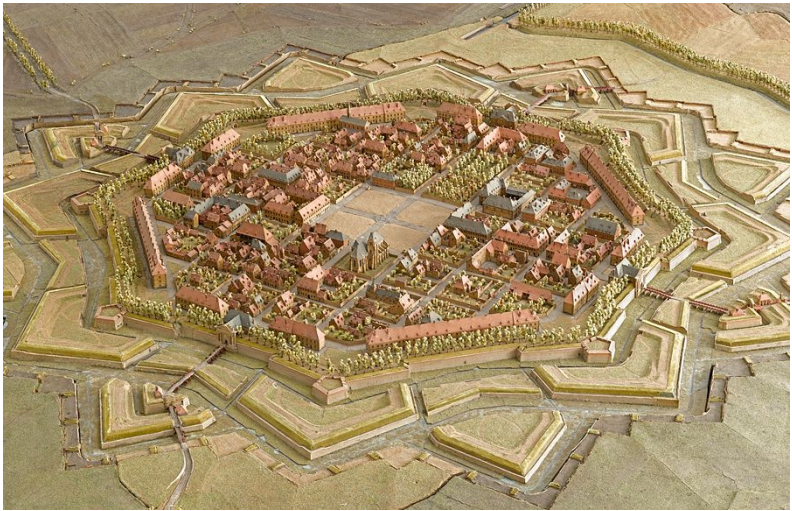
Transition en trois phases



Transition en trois phases



Phase 1 : défense en profondeur



Phase 1 : défense en profondeur

- Les algorithmes post-quantiques **doivent être hybridés** avec des algorithmes classiques déjà reconnus.
  - ☞ (exception : signatures basées sur le hachage).
- La sécurité post-quantique est **recommandée** pour les données de longue durée de vie.

- Les implémentations disposent d'une relative *liberté* quant au choix de l'algorithme post-quantique :
  - ☞ (mais il est préférable d'utiliser une spécification *stable* et *bien comprise*).
  - ☞ (Liste de recommandations dans les prochaines planches).
- L'hybridation est obligatoire pour les produits complets, mais les composants ou librairies peuvent bien sûr être spécialisés pour les algorithmes post-quantiques.
- Il est recommandé d'utiliser un niveau de sécurité post-quantique correspondant à celui des primitives symétriques
  - ☞ au moins NIST niveau 3 $\approx$ AES192, idéalement NIST level 5 $\approx$ AES256.

Phase 2: confiance en la résistance post-quantique

Phase 2: confiance en la résistance post-quantique

- L'hybridation **reste obligatoire**.
- Certains mécanismes fournissent une **assurance de sécurité** post-quantique.
- La sécurité post-quantique sera **vivement recommandée** pour la sécurité à long terme.

- L'ANSSI établit une liste de *critères* pour les algorithmes post-quantiques.
- Les algorithmes recommandés sont (pour l'instant) ceux du NIST et FrodoKEM.
- L'hybridation continue de garantir la non-régression.

Date de début : après 2025.

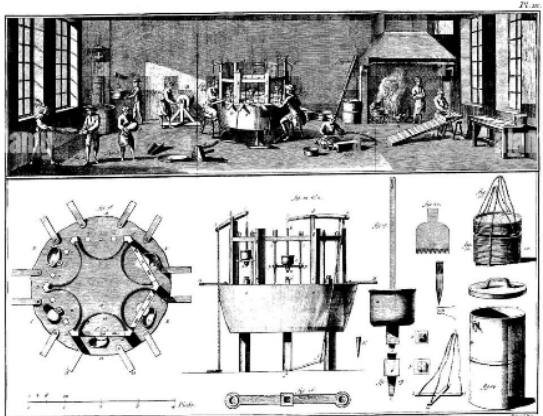
Phase 3: cryptographie post-quantique autonome

Phase 3: cryptographie post-quantique autonome

- Certains algorithmes post-quantiques sont reconnus **sans hybridation**.
- La sécurité post-quantique devient **obligatoire** au moins dans certains cas.

Date de début : probablement après 2030.

3. Recommandations techniques



Epinglier

3. Recommandations techniques

Primitives post-quantiques

Échange de clés basé sur les réseaux

ML-KEM (CRYSTALS-Kyber)	FrodoKEM
Réseaux structurés	Réseaux non structurés
Efficace pour la plupart des usages	Moins efficace
	Meilleure confiance

Recommandations:

- *Ne pas dévier* des versions standardisées.
- Choisir au moins ML-KEM-768 ou FrodoKEM-976 ($\approx$ AES192), préférablement ML-KEM-1024 ou FrodoKEM-1344 ($\approx$ AES256).
- Échanger des *clés éphémères* si possible : ceci empêche par exemple les attaques par échec du déchiffrement.
- Implémenter la version *sûre contre un attaquant actif (IND-CCA)* documentée dans le processus NIST.

Signatures basées sur les réseaux

ML-DSA (CRYSTALS-Dilithium)	FN-DSA (FALCON)
Réseaux structurés	Réseaux structurés
Rapide	Plus compact
Construction simple	Arithmétique flottante

Recommandations:

- *Ne pas dévier* des versions standardisées.
- Choisir au moins ML-DSA-65 ($\approx$ AES192), préférablement ML-DSA-87 ($\approx$ AES256).
- Pour FALCON :
  - Choisir FALCON-1024 ($\approx$ AES256).
  - *Ne pas modifier* les distributions gaussiennes, qui jouent un rôle important dans la preuve de sécurité.
  - La sécurité de FALCON contre les attaques par canaux auxiliaires est délicate à assurer.

Signatures basées sur le hachage

- Ces algorithmes reposent sur une *preuve de sécurité* ramenant leur sécurité à certaines caractéristiques de fonctions de hachage.
- Ils peuvent déjà être utilisés **sans hybridation** à condition de respecter les conditions de la preuve de sécurité.

- Les performances nécessitent de faire des choix :
  - algorithmes généralistes avec une taille de signature importante (par ex. SPHINCS+-SHA2-128f: 17 ko);
  - algorithmes **à état** avec un nombre **borné** de signatures par clé privée.
- Les cas d'usages réalistes sont restreints :
  - mises à jour logicielles : (infréquentes, intrinsèquement à état, non contraint en taille, vulnérables aux attaques rétroactives).
  - identité numérique.

Signatures basées sur le hachage

XMSS, LMS	SPHINCS+
à état	variante **sans état** de XMSS
Nombre restreint de signatures	Signatures plus volumineuses Moins efficace

- Ces trois schémas sont considérés comme des *choix prudents* et peuvent être utilisés **sans hybridation**.
- *Ne pas dévier* des versions standardisées.
- Choisir des fonctions de hachage d'au moins 192 bits, préférablement 256 bits.
- L'état associé à une clé privée XMSS/LMS est **critique** et doit être géré de manière sûre.
  - L'état doit être protégé en *intégrité* et contre la réutilisation.
  - Ceci empêche notamment la redondance du stockage de la clé privée.

3. Recommandations techniques

Position sur les mécanismes d'hybridation

“Hybridation du pauvre”: clés pré-partagées

Algorithme pré-quantique + clé (symétrique) pré-partagée.

- Mesure **provisoire**.
- La sécurité **(confidentialité et intégrité)** de la clé pré-partagée est cruciale.
- Chaque clé ne peut être pré-partagée qu’entre *deux* entités.
- Pas de PFS (sécurité persistante) intrinsèque contre les adversaires quantiques.

Confidentialité : combineurs de clés

- Protocole combinant plusieurs échanges de clé (post-quantiques ou non) en un seul échange.
- Sécurité IND-CPA : l'échange combiné est IND-CPA dès qu'**au moins l'un** des échanges individuels l'est.
  - (idem pour IND-CCA).
  - Recherche encore active sur les preuves de sécurité !

	IND-CPA	IND-CCA	
CAT	✗	✗	
XOR	✓	✗	
XOR-then-PRF	✓	(✗)	
Dual-PRF	✓	(✓)	
CAT-then-KDF	✓	(✓)	TLS v1.3 draft
CASCADE	✓	(✓)	IKEv2 draft (RFC9370)

Authenticité : combineur de signatures

La combinaison de signatures par concaténation est sûre au sens EUF-CMA.

Le vérifieur **doit** vérifier les deux signatures.

- Au niveau protocolaire, il est possible de définir un nouvel « algorithme combiné » ou de vérifier individuellement les deux signatures.
  - ☞ Deux signatures dans un seul certificat X.509 ou dans deux certificats ?
- Pas d'impact sur la sécurité, l'arbitrage se fait au niveau des protocoles.

Questions ?