Sensibilisation à la cryptographie post-quantique

ou

Comment la cryptographie post-quantique peut-elle faire barrage pour résister à la montée en puissance des ordinateurs quantiques ?

Par Thierry Gayet

Septembre 2025
Association LinuxMaine
72000 LE MANS

Compte-rendu rédigé par
JMV avec l'aide de l'IA

Table des matières

Préambule

Ce document se veut un compte-rendu de la présentation du Samedi 13 Septembre 2025 faite par Thierry Gayet dans les locaux de l'association mancelle LinuxMaine.

Le sujet en est : **Sensibilisation à la cryptographie post-quantique** ou *« Comment la cryptographie post-quantique peut-elle faire barrage pour résister à la montée en puissance des ordinateurs quantiques ? »*

Évidemment la question du temps d'exécution des algorithmes est essentielle ainsi que celle du chiffrement des données. À ce titre le chiffrement RSA a d'ailleurs été maintes fois évoqué ainsi que la notion théorique de complexité des algorithmes.

Dans le but d'aider à la compréhension de ces sujets nous recommandons donc la lecture de deux documents mis en ligne sur le site de LinuxMaine :

1. *Le chiffrement RSA sous Thunderbird*, qui fournit un éclairage sur le fonctionnement du chiffrement RSA ainsi que son implémentation avec Thunderbird comme client de messagerie.

2. *Complexité des algorithmes* qui apporte quelques éléments de *Théorie de la Complexité*. En commençant par la notion de complexité d'un algorithme (complexité en temps d'exécution et dans le pire des cas selon l'expression consacrée), le document fait un un passage par les *machines de Turing*, ces modèles théoriques d'ordinateurs, qui permettent de définir les classes P et NP de problèmes. Ce sera l'occasion de donner quelques exemples de problèmes réputés difficiles pour toucher du doigt la véritable problématique du temps d'exécution.
   Il est difficile aussi de passer sous silence la classe des problèmes *NP-Complets* qui focalisent beaucoup d'attention puisque la théorie assure qu'en résoudre un seul permettrait de résoudre tous les autres *sans trop d'efforts*.

Nous débutons par un examen des enjeux et des menaces que les ordinateurs quantiques ainsi que les algorithmes du même nom font peser sur la cryptographie actuelle.

Nous présentons ensuite ordinateurs et algorithme quantiques avant de nous attarder sur leur fonctionnement.

Finalement, l 'accent sera mis plus particulièrement sur la **cryptographie post-quantique** comme une réponse « quantique-résistante ».

A Constat

A.1 Contexte et Enjeux

Le tableau ci-dessous[1] donne une idée du temps nécessaire à un algorithme qui effectue une recherche exhaustive[2] pour trouver un mot de passe.

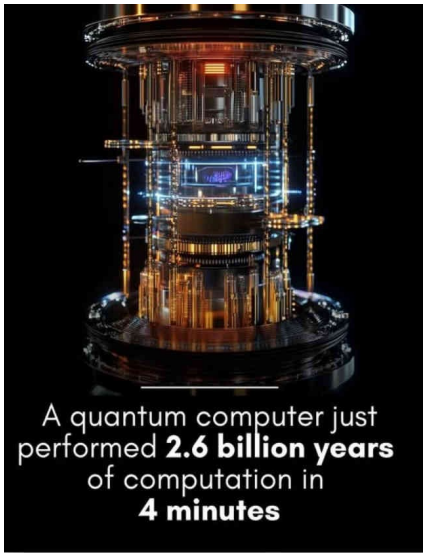
Combien de temps faut-il à un pirate pour trouver votre mot de passe 2025

12 x RTX 5090 | bcrypt (10)

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	57 minutes	2 heures	4 heures
6	Instantané	46 minutes	2 jours	6 jours	2 semaines
7	Instantané	20 heures	4 mois	1 an	2 ans
8	Instantané	3 semaines	15 ans	62 ans	164 ans
9	2 heures	2 ans	791 ans	3k ans	11k ans
10	1 jour	40 ans	41k ans	238k ans	803k ans
11	1 semaine	1k ans	2M ans	14M ans	56M ans
12	3 mois	27k ans	111M ans	917M ans	3Md ans
13	3 ans	705k ans	5Md ans	56Md ans	275Md ans
14	28 ans	18M ans	300Md ans	3Bn ans	19Bn ans
15	284 ans	477M ans	15Bn ans	218Bn ans	1Bd ans
16	2k ans	12Md ans	812Bn ans	13Bd ans	94Bd ans
17	28k ans	322Md ans	42Bd ans	840Bd ans	6Tn ans
18	284k ans	8Bn ans	2Tn ans	52Tn ans	463Tn ans

Hive Systems › hivesystems.com/password

En seulement 4 minutes, l'ordinateur quantique chinois à 76 qubits a résolu un problème qui aurait pris des milliards d'années au supercalculateur le plus rapide.



La cryptographie est essentielle pour protéger la confidentialité, l'intégrité et l'authenticité des données dans la société numérique (banque, messagerie, blockchain, etc.).

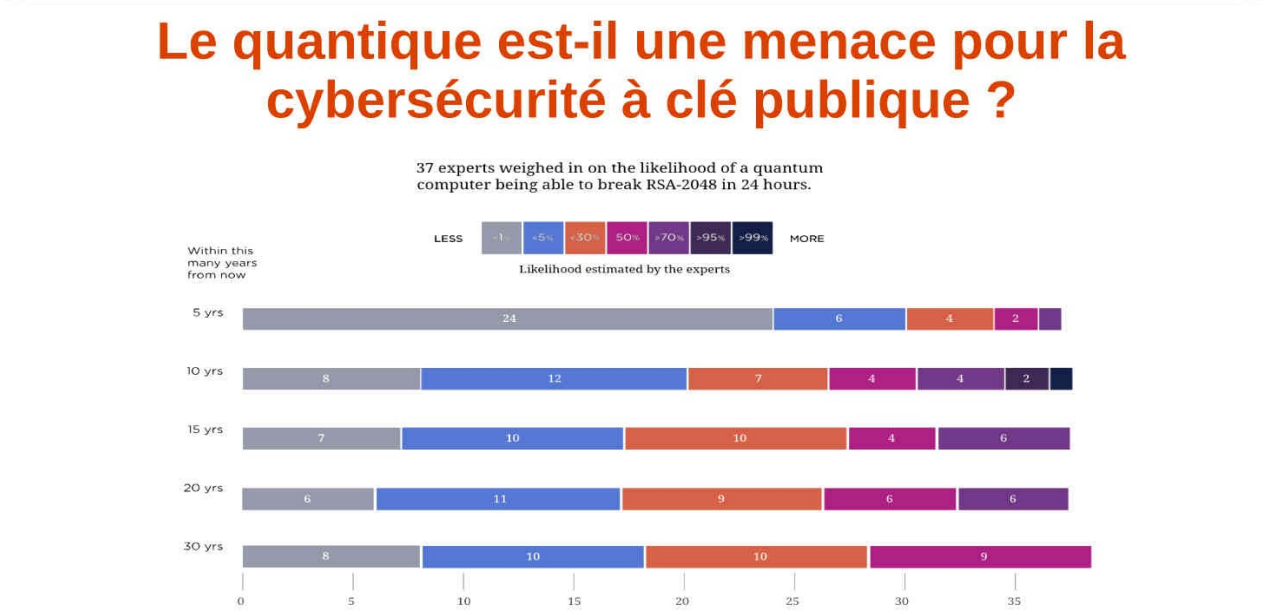
Les ordinateurs quantiques menacent les systèmes cryptographiques actuels (RSA, ECC, Diffie-Hellman) en rendant possibles des attaques jusqu'alors impossibles avec des ordinateurs classiques, grâce à des algorithmes comme ceux de **Shor** (factorisation) et **Grover** (recherche).

1 https://www.francenum.gouv.fr/magazine-du-numerique/combien-de-temps-un-pirate-met-il-pour-trouver-votre-mot-de-passe-comment

2 https://fr.wikipedia.org/wiki/Recherche_exhaustive

A.2 Menaces et risques selon les experts.

- **Exemple concret :** Un ordinateur quantique pourrait casser une clé RSA-2048 en moins de 24 heures d'ici 20 à 30 ans, selon l'opinion d'un majorité d'experts.



- **Attaques rétroactives** ("store now, decrypt later") : Des données chiffrées aujourd'hui pourraient être déchiffrées demain par des ordinateurs quantiques.
- **Impact** : Effondrement de la sécurité des infrastructures numériques (banques, gouvernements, communications privées).
- **État actuel** : Les ordinateurs quantiques existent, mais restent expérimentaux. Cependant, des agences comme la NSA investissent massivement dans cette technologie.

- **Conclusion générale :**
    - Court terme (5–10 ans) : RSA-2048 est jugé sûr, très peu croient à une menace réelle.
    - Moyen terme (15–20 ans) : les avis sont très partagés, signe d'incertitude
    - Long terme (30 ans) : la majorité estime probable ou très probable qu'un ordinateur quantique puisse casser RSA-2048 en une journée.
- **En résumé :**
    - Pas de risque immédiat, mais forte incertitude à 15–20 ans et probabilité à 30 ans.
    - Cela renforce l'idée que les systèmes cryptographiques doivent commencer à migrer progressivement vers des algorithmes résistants au quantique (post-quantum cryptography).

B Ordinateurs et algorithmes quantiques

B.1 Physique Quantique : Fondements

B.1.a Concepts Clés

- **Quantification** : Certaines propriétés physiques (comme l'énergie d'un électron) ne peuvent prendre que des valeurs discrètes, et non continues.

- **Dualité onde-corpuscule** : Les particules (ex. : photons) se comportent à la fois comme des ondes et des particules.

- **Superposition** : Une particule peut exister dans plusieurs états simultanément jusqu'à ce qu'une mesure soit effectuée (ex. : le chat de Schrödinger, à la fois mort et vivant). *Un qubit peut être 0 et 1 simultanément.*

- **Intrication quantique** : L'état de deux particules intriquées est corrélé, même à distance. Mesurer l'état de l'une détermine instantanément l'état de l'autre, quelle que soit la distance.

B.1.b Applications en Cryptographie

- **Distribution Quantique de Clés (QKD)** : Des protocoles comme **BB84** ou **E91** utilisent la superposition et l'intrication pour échanger des clés de manière sécurisée. Toute tentative d'espionnage modifie l'état des photons, révélant la présence d'un intrus[3].

B.1.c Menaces sur la Cryptographie actuelle

Algorithmes Vulnérables

- **Asymétrique** :
    - **RSA, ECC, Diffie-Hellman** : Cassés par l'algorithme de Shor.

      Impact : Signature numérique, échange de clés, TLS/SSL.
- **Symétrique** :
    - **AES** : Résiste à Grover si la taille de clé est doublée (ex. : AES-256 → sécurité équivalente à AES-128 face à un attaquant classique).

Scénarios d'attaque

- **"Store Now, Decrypt Later"** : Stockage de données chiffrées aujourd'hui pour les déchiffrer plus tard avec un ordinateur quantique.
- **Attaques rétroactives** : Compromission de communications passées (ex. : emails, transactions bancaires).

Algorithmes, complexité et résistance au quantique

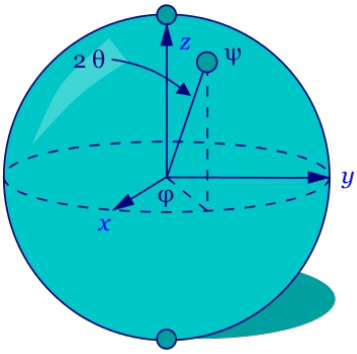
Calcul	Complexité (ordinateur classique)	Temps d'accès	Résistant au quantique
Accès à un tableau	$O(1)$	$10\,ns$	Oui
Parcours d'une liste	$O(n)$	$10\,\mu s$	Oui
Factorisation	$O(2^{poly(n)})$	$10^{20}\,ans$	Non (Shor)
Problème du voyageur de commerce	$O(n!)$	Pas mesurable	Oui

3 Ce sujet est traité dans les diapositives 26 et 27.

C Ordinateurs Quantiques : Fonctionnement

C.1 Qubits

- **Définition** : Unité de base de l'information quantique, pouvant être dans un état de superposition de 0 et 1, représenté par : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ où α et β sont des amplitudes de probabilité (nombres complexes).



Grâce à la propriété de superposition quantique, un qubit stocke une information qualitativement différente de celle d'un bit. D'un point de vue quantitatif, un qubit peut être dans une multitude d'états combinaison linéaire de la forme $\alpha|0\rangle + \beta|1\rangle$ avec α et β, des nombres complexes vérifiant : $|\alpha|^2 + |\beta|^2 = 1$.

Tout se passe comme si les états quantiques d'un qubit se trouvaient à la surface d'une sphère de rayon 1.

- **Mesure** : La mesure d'un qubit donne 0 avec une probabilité $|\alpha|^2$ et 1 avec une probabilité $|\beta|^2$.

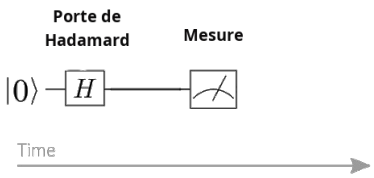
C.2 Portes Quantiques

- **Rôle** : Elles manipulent les qubits pour effectuer des calculs.
- **Exemples :**
  - **Porte de Hadamard (H)** : Crée une superposition.
    Cas particulier porte H_1 : Une porte de Hadamard H_1 est une opération quantique fondamentale qui agit sur un seul qubit. Voici ce qu'elle fait :
    Si le qubit d'entrée est à l'état $|0\rangle$ le qubit de sortie est à l'état $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$.
    Si le qubit d'entrée est à l'état $|1\rangle$ le qubit de sortie est à l'état $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.
    Vu que $|\alpha| = |\beta| = \frac{1}{\sqrt{2}}$ et que $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$, les deux états $|0\rangle$ et $|1\rangle$ sont équiprobables à la sortie.
  - **Porte CNOT** : Crée une intrication entre deux qubits.
  - **Portes de Pauli (X, Y, Z)** : Modifient l'état ou la phase du qubit.

C.3 Circuit quantique :

C'est une séquence de portes appliquées à des qubits pour résoudre des problèmes (ex.: factorisation).

Exemple : Un circuit quantique pour simuler un tirage au sort (pile ou face).



[En fait la production de nombres aléatoires avec un ordinateur classique n'avait rien d'aléatoire. Il s'agissait d'un calcul parfaitement déterministe réalisé à partir d'une *graine*. L'illusion de l'aléa venait du choix de la graine (heure système, mouvements de souris, …)].

C.4 Algorithmes Quantiques

- **Algorithme de Shor** :
    - **Fonction** : Factorise de grands nombres en temps polynomial, c'est une menace pour RSA et ECC.
    - **Impact** : Rend obsolètes les systèmes de chiffrement asymétrique actuels.

- **Algorithme de Grover** :
    - **Fonction** : Accélère la recherche non structurée (ex. : force brute sur AES).
    - **Impact** : Réduit la sécurité de moitié (ex. : AES-128 devient équivalent à AES-64 face à Grover).

C.5 Bibliothèques Disponibles

- **python3-pqcrypto** : Pour tester ML-KEM, Dilithium, etc.
- **PyCryptodrome** : Benchmarking des algorithmes de cryptographie post-quantique.

C.6 Ressources et Références

- **Normes NIST** :
    - NIST PQC Standardization Process

- **Outils** :
    - GitHub - pqcrypto
    - OpenSSH 10.0 Release Notes

- **Articles Techniques** :
    - Comment fonctionne la cryptographie quantique ?

D Cryptographie Post-Quantique (PQC)

D.1 Définition

- Ensemble d'algorithmes conçus pour résister aux attaques quantiques, tout en étant implémentables sur des ordinateurs classiques.

D.2 Différence avec la cryptographie quantique

- La PQC utilise des mathématiques avancées, tandis que la cryptographie quantique repose sur des principes physiques (ex. : distribution quantique de clés, QKD).

D.3 Algorithmes Standardisés par le NIST (2024)

- **ML-KEM** (ex-Kyber) : Échange de clés post-quantique, utilisé par défaut dans OpenSSH 10.0.
- **ML-DSA** (ex-Dilithium) et **SLH-DSA** (ex-SPHINCS+) : Signatures numériques résistantes au quantique.
- **FN-DSA** (ex-Falcon) : Alternative pour les signatures, en cours de finalisation.

D.4 Familles d'Algorithmes PQC

- **Problèmes Mathématiques Résistants**

  La Cryptographie post-quantique repose sur des problèmes considérés comme difficiles même pour un ordinateur quantique :
- **Réseaux euclidiens** :
  - **LWE (Learning With Errors)** : Distinguer une distribution bruitée d'une distribution aléatoire.
  - **SIS (Short Integer Solution)** : Trouver un vecteur court dans un réseau.

    Exemples : Kyber, Dilithium.
- **Codes correcteurs d'erreur** :
  - **Problème du décodage de syndrome** : Retrouver un mot de code à partir d'un syndrome.
    Exemple : Classic McEliece.
- **Polynômes multivariés** :
  - Résolution de systèmes d'équations non linéaires.

    Exemple : Rainbow (cassé en 2022).
- **Isogénies de courbes elliptiques** :
  - Trouver une isogénie entre deux courbes supersingulières.

    Exemple : SIKE (cassé en 2022).
- **Hachage**
  - SPHINCS+
  - Sécurité forte, mais signatures lentes/volumineuses

D.5 Exemple : ML-KEM (Kyber)

- **Fonctionnement** :
  - Échange de clefs basé sur le problème **LWE**.

    Combinaison de matrices et vecteurs avec du bruit pour garantir la sécurité.
- **Performances** :
  - **Rapide** : Plusieurs centaines de fois plus rapide que RSA-4096.
  - **Taille des clés** : 1,5 Ko pour Kyber-1024 (vs 256 octets pour RSA-2048).
- **Intégration** :
  - Déjà utilisé dans **OpenSSH 10.0** (algorithme hybride `mlkem768x25519-sha256`).
- **Plus de détails sur le problème LWE :**

  Le problème **LWE** (pour *Learning With Errors*) est un problème mathématique central en cryptographie post-quantique. Le LWE consiste à résoudre un système d'équations linéaires bruitées dans un espace vectoriel fini.
  Plus précisément :
  - On part d'une matrice aléatoire **A** et d'un vecteur secret **s**.
  - On calcule des produits scalaires entre les lignes de **A** et **s**, puis on ajoute un petit bruit aléatoire (erreur) à chaque résultat.
  - Le défi : retrouver le vecteur secret **s** à partir de ces équations bruitées.
  - **Pourquoi est-ce important ?**
    - **Sécurité post-quantique** : Le LWE est considéré comme résistant aux attaques des ordinateurs quantiques, contrairement à des problèmes comme la factorisation ou le logarithme discret.
    - **Base de nombreux schémas cryptographiques** : Il sert à construire des systèmes de chiffrement, des signatures numériques, etc., sécurisés contre les attaques quantiques.
  - **Exemple simplifié**
    Imaginez que vous avez :
- Une équation du type : $3 \times s1 + 2 \times s2 + bruit = 5$

    Votre but : retrouver s1 et s2 malgré le bruit.
  - **Difficulté du problème**
    La sécurité repose sur le fait qu'il est très difficile de distinguer les équations bruitées de véritables équations aléatoires, même pour un ordinateur quantique.
  - **Applications**
    - Chiffrement (ex : Kyber, un algorithme standardisé par le NIST).
    - Signatures numériques (ex : Dilithium).

En résumé, le LWE est un pilier de la cryptographie moderne, car il offre une sécurité robuste face aux futures menaces quantiques.

D.6 Comparaison des Performances

- **ML-KEM** (post-quantique) est **beaucoup plus rapide que RSA**, mais moins rapide qu'AES (symétrique).
- **Taille des clés** : Les algorithmes PQC ont des clés plus grandes que RSA/ECC (ex. : 1,5 Ko pour Kyber-1024 vs 256 octets pour RSA-2048).
- **Adoption** : OpenSSH 10.0 utilise déjà ML-KEM par défaut pour l'échange de clés.

Comparaison : Cryptographie Classique vs Post-Quantique

Critère	Cryptographie Classique	Cryptographie Post-Quantique
Sécurité	Basée sur la factorisation	Basée sur des réseaux, hachage, etc.
Résistance quantique	Non	Oui
Taille des clés	Compacte (ex. RSA-2048 : 256 B)	Plus grande (ex. Kyber : 1,5 KB)
Performance	Rapide (RSA, ECC)	Variable (rapide pour Kyber)

D.7 Recommandations et Transition

- **Urgence** : Commencer la migration vers la PQC dès maintenant pour éviter les risques futurs.
- **ANSSI et NIST** encouragent l'adoption progressive des algorithmes PQC dans les infrastructures critiques.
- **Outils disponibles** : Bibliothèques comme `python3-pqcrypto` pour tester et implémenter ces algorithmes.

D.8 Exemples Concrets

- **Bitcoin** : Devra remplacer ECDSA par un algorithme résistant au quantique si les ordinateurs quantiques deviennent une menace.
- **OpenSSH** : Intègre déjà des algorithmes hybrides (ML-KEM + X25519) pour une sécurité renforcée.

E Conclusion

La cryptographie post-quantique est une **nécessité** pour sécuriser les données face à la menace quantique. Les algorithmes comme **Kyber** et **Dilithium** sont déjà standardisés et déployés, mais la transition doit s'accélérer pour éviter des failles critiques. La sensibilisation et l'adoption par les acteurs industriels et gouvernementaux sont essentielles.