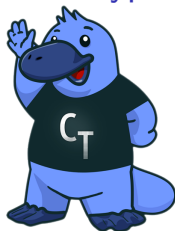


# Introduction à la cryptographie Post-Quantique



Pascal Lafourcade



Clermtontech 17 Septembre 2025

# Qubit dans les années 80 ... Benjamin Schumacher 1995

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \text{ avec } (\alpha, \beta) \in \mathbb{C}, \text{ tel que } \alpha|0\rangle + \beta|1\rangle = 1$$
$$||\psi||^2 = |\alpha|^2 + |\beta|^2 = \alpha \cdot \bar{\alpha} + \beta \cdot \bar{\beta} = 1$$

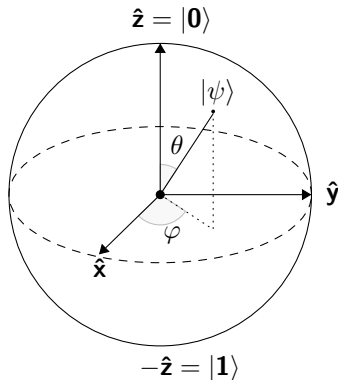


1

0



1



# Ordinateurs quantiques

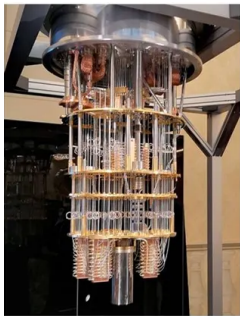


- 1998 : 2 qbits, IBM
- 1999 : 3 qbits, IBM
- 2001 : 7 qbits, IBM
- 2017 : 50 qbits, IBM Q50
- 2019 : 53 qbits, Google Sycamore
- 2021 : 90 qbits, Rigetti Aspen-9
- 2021 : 127 qbits, IBM Eagle
- 2022 : 433 qbits, IBM Osprey
- Dec 2023 : 1 121 qubits, IBM Condor



- 2011 : 128 qbits, One
- 2013 : 512 qbits, Two
- 2015 : 1152 qbits, 2X
- 2017 : 2048 qbits, 2000Q
- 2020 : 5760 qbits, Advantage
- 2024 : 7440 qubits, Advantage 2

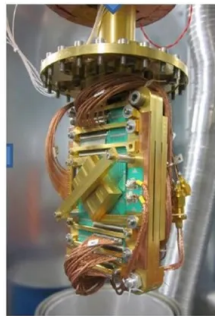
# Ordinateurs quantiques



IBM



rigetti



D:wave

# Portes quantiques

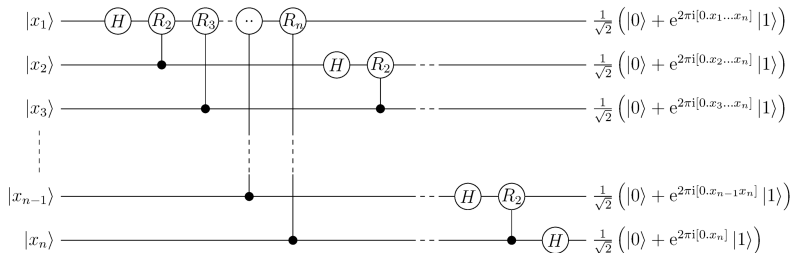
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

# Circuits quantiques



Transformée de Fourier quantique

# Algorithmes quantiques

- Algorithme de Deutsch (1985) et Deutsch-Jozsa (1992)
- Algorithme de Simon (1994)
- Algorithme de Shor (1994)
- Algorithme de Grover (1996)



# Shor et Grover

## Algorithme de Shor (1994)

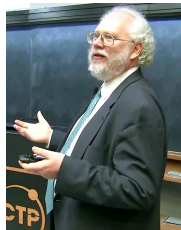
Calcule l'ordre d'un nombre en temps polynomial.

## Définition de l'ordre

L'ordre de  $a$  est le plus petit entier  $r$  tel que  $a^r \equiv 1 \pmod{N}$

## Algorithme de Grover (1996)

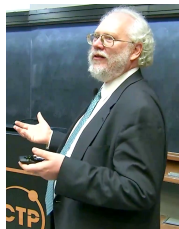
Trouver efficacement un élément qui satisfait une propriété dans une liste donnée.



# Plan

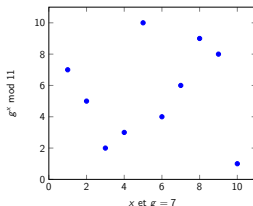
1. Ordinateur quantique
2. Impact de l'ordinateur quantique sur la cryptographie
3. Cryptographie Post-Quantique
4. Conclusion

# Cryptographie Pré-quantique



Deux problèmes :

- Factorisation :  $n = p \times q$  difficile de trouver  $p$  et  $q$ .
- Logarithme discret :  $g, p, g^x \bmod p$  difficile de trouver  $x$ .

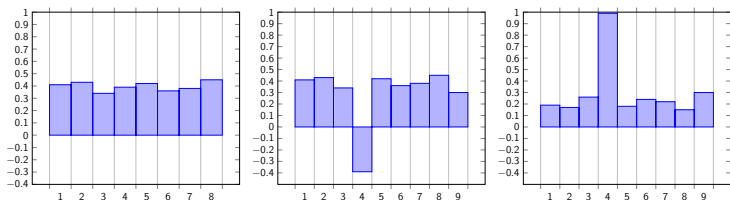


C'est deux problèmes sont cassés par l'algorithmes de **Shor** !

**“Store-now, decrypt-later”**



Trouver  $x \in \{0,1\}^n$  avec  $F(x)$  en  $\sqrt{2^n}$  évaluations de  $F$



Oracle quantique qui détermine  $x$

Diminue légèrement la sécurité pour :

- les fonctions de hachages de  $O(2^{\frac{N}{2}})$  à  $O(2^{\frac{N}{3}})$
- les chiffrements symétriques de  $O(2^n)$  à  $O(2^{\frac{n}{2}})$

# Plan

1. Ordinateur quantique
2. Impact de l'ordinateur quantique sur la cryptographie
3. Cryptographie Post-Quantique
4. Conclusion

# Cryptographie Post-Quantique



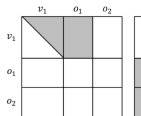
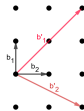
- Fonctionne sur les ordinateurs classiques
- Résiste à un ordinateur quantique



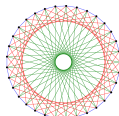
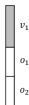
Les problèmes difficiles sous-jacents sont différents !

# 5 familles de problèmes difficiles

- Fonctions de hachage
- Réseaux Euclidiens (Lattices)
- Codes
- Systèmes Multivariés
- Isogénies



=



# Compétition du NIST lancée en 2017



- 30 novembre 2017 : 69 sousmissions Round 1
- 30 janvier 2019 : 26 sousmissions choisies pour le Round 2
- 22 juillet 2020 : 7+8 sousmissions choisies pour le Round 3
- 5 juillet, 2022 :
  - KEM : Kyber
  - Signature : Dilithium, Falcon, SPHINCS+
- 13 août 2024, NIST publie les standards :
  - FIPS 203 (Kyber),
  - FIPS 204 (Dilithium)
  - FIPS 205 (SPHINCS+)
  - FIPS 206 (FALCON à venir)
- 10 mars 2025, NIST annonce le vainqueur du Round 4 : KEM HQC



# Autres compétitions

## Corée du Sud (2016 - 2018), 2025 (Lattice based)

- KEM : SMAUG-T et NTRU+
- DSA : AIMer et HAETAE (Similaire à Dilithium).

## Chine, 3 janvier 2020 (Lattice based)

- Aigis-sig et Aigis-enc
- LAC.PKE

## Ukraine a standardisé (Lattice based)

- KEM : DSTU 8961:2019 Skelya, proche de CRYSTALS-KYBER.
- Signature : Falcon

## Russie 2019 -

- KEM : FORZITSIYA (forsythia) et LIMMONITSA (citronelle) (Isogénies)
- Signature : SHIPOVNIK (églatine) et KRYZHOVNIK (groseille à maquereau) une variante optimisée de Dilithium.

# Plan

1. Ordinateur quantique
2. Impact de l'ordinateur quantique sur la cryptographie
3. Cryptographie Post-Quantique
4. Conclusion

# Changements en cours

- 2014 : La Fondation Linux a créé la Post-Quantum Cryptography Alliance (PQCA)

- Septembre 2023 : PQXDH protocol (Signal)



- Février 2024 : PQ3 protocol (imessage)



- Avril 2024 :  Chrome > 124 utilise Kyber768 pour TLS 1.3

- Mai 2024 :  migre vers Kyber pour l'échange de clés TLS.

- Le 7 juin 2024,  ont proclamé 2025 comme l'Année Internationale de la Science et de la Technologie Quantiques

- Février 2025 :  annonce 1 million de qbits topologiques, Majorana



- Le 10 juin 2025,  annonce Quantum Starling pour 2029 !

# Hybridation



Le meilleur des deux mondes

- ML-KEM : CRYSTALS-Kyber
- KEM : HQC
- ML-DSA : CRYSTALS-Dilithium
- SLH-DSA : SPHINCS+
- FN-DSA : Falcon

|             | Taille en bytes |         | Temps en cycles |               |
|-------------|-----------------|---------|-----------------|---------------|
|             | Clé publique    | Chiffré | Encapsulation   | Décapsulation |
| ML-KEM-512  | 800             | 2 420   | 45 200          | 34 572        |
| HQC-KEM 256 | 7 245           | 14 485  | 753 000         | 1 469 000     |
| RSA         | 512             | 512     | 400 000         | 4 000 000     |

|         | Taille en bytes |           | Temps en cycles |              |
|---------|-----------------|-----------|-----------------|--------------|
|         | Clé publique    | Signature | Signature       | Vérification |
| ML-DSA  | 1 312           | 2 420     | 333 013         | 118 412      |
| FN-DSA  | 897             | 666       | 386 678         | 82 340       |
| SLH-DSA | 32              | 17 088    | 1 100 000 000   | 1 190 000    |
| DSA     | 521             | 64        | 4 000 000       | 400 000      |

# A retenir



Novembre 2024

| Algorithmes | Transition          |
|-------------|---------------------|
| ECDSA       | Déprécié après 2030 |
|             | Interdit après 2035 |
| RSA         | Déprécié après 2030 |
|             | Interdit après 2035 |

# Conclusion

Merci pour votre attention



pascal.lafourcade@uca.fr