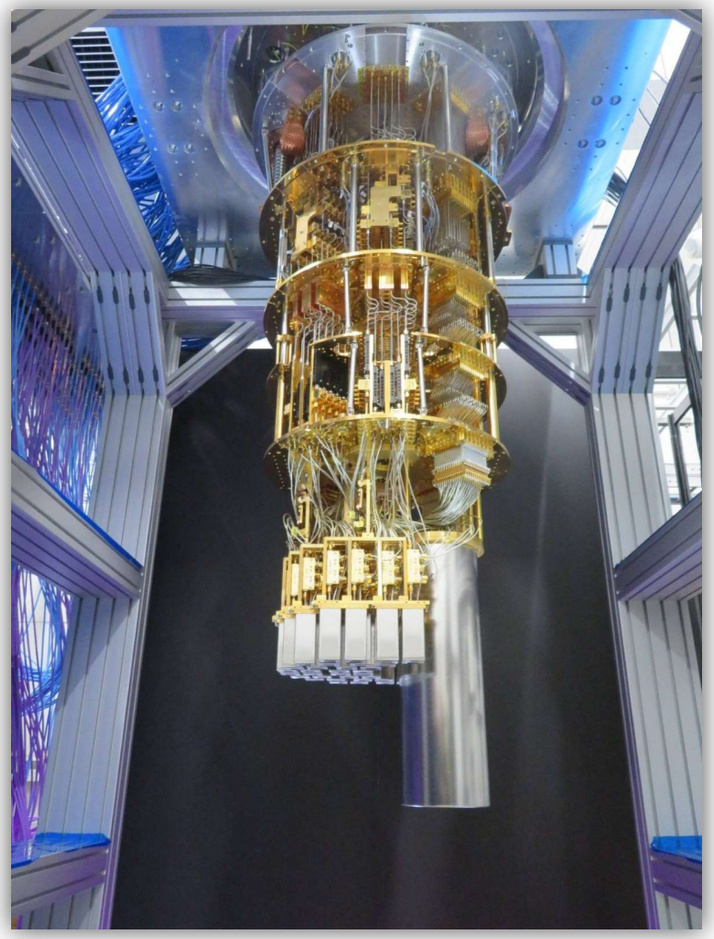
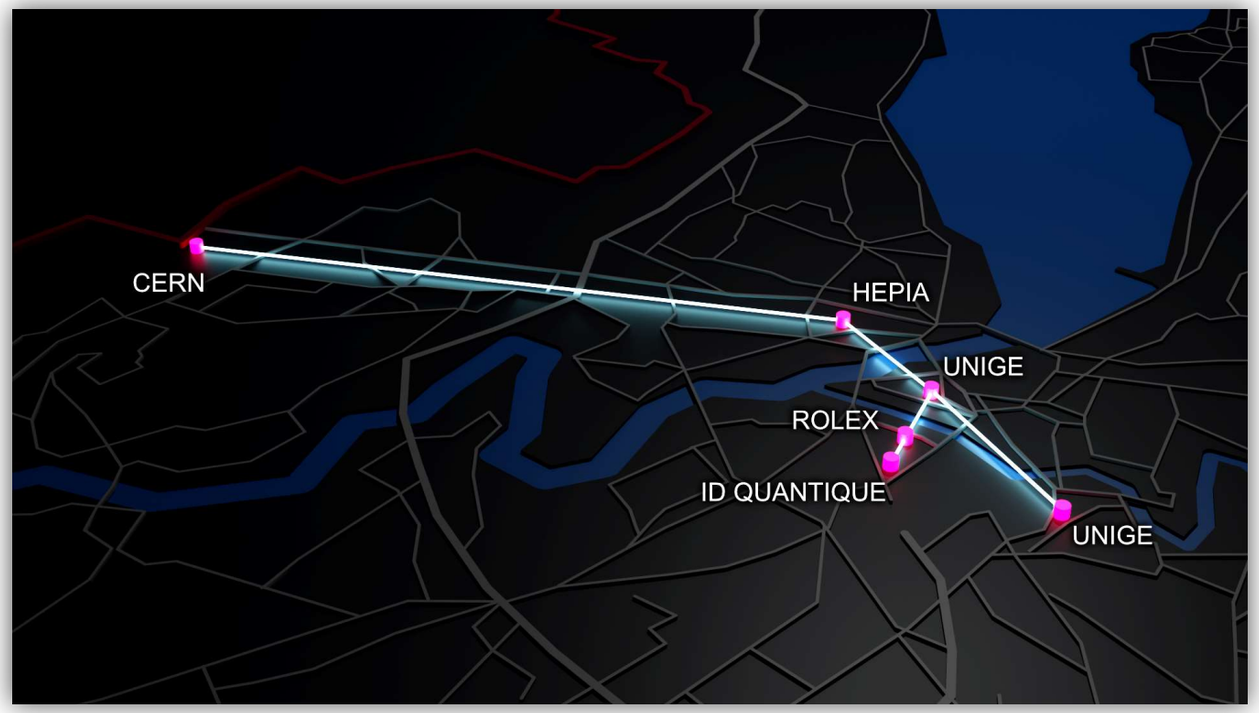
Qu'est-ce que l'informatique quantique ?

Novembre 2025



ordinateur quantique de Fujitsu et institut Riken (avril 2025)

Actualité !



Geneva Quantum Network (illustration Xavier Ravinet, octobre 2025)

Nobel Prize in Physics 2025

Ill. Niklas Elmehed © Nobel Prize Outreach

John Clarke

Prize share: 1/3

Ill. Niklas Elmehed © Nobel Prize Outreach

Michel H. Devoret

Prize share: 1/3

Ill. Niklas Elmehed © Nobel Prize Outreach

John M. Martinis

Prize share: 1/3

The Nobel Prize in Physics 2025 was awarded jointly to John Clarke, Michel H. Devoret and John M. Martinis "for the discovery of macroscopic quantum mechanical tunnelling and energy quantisation in an electric circuit"

Académie royale des sciences de Suède (octobre 2025)

Sommaire

Introduction

L'informatique quantique...

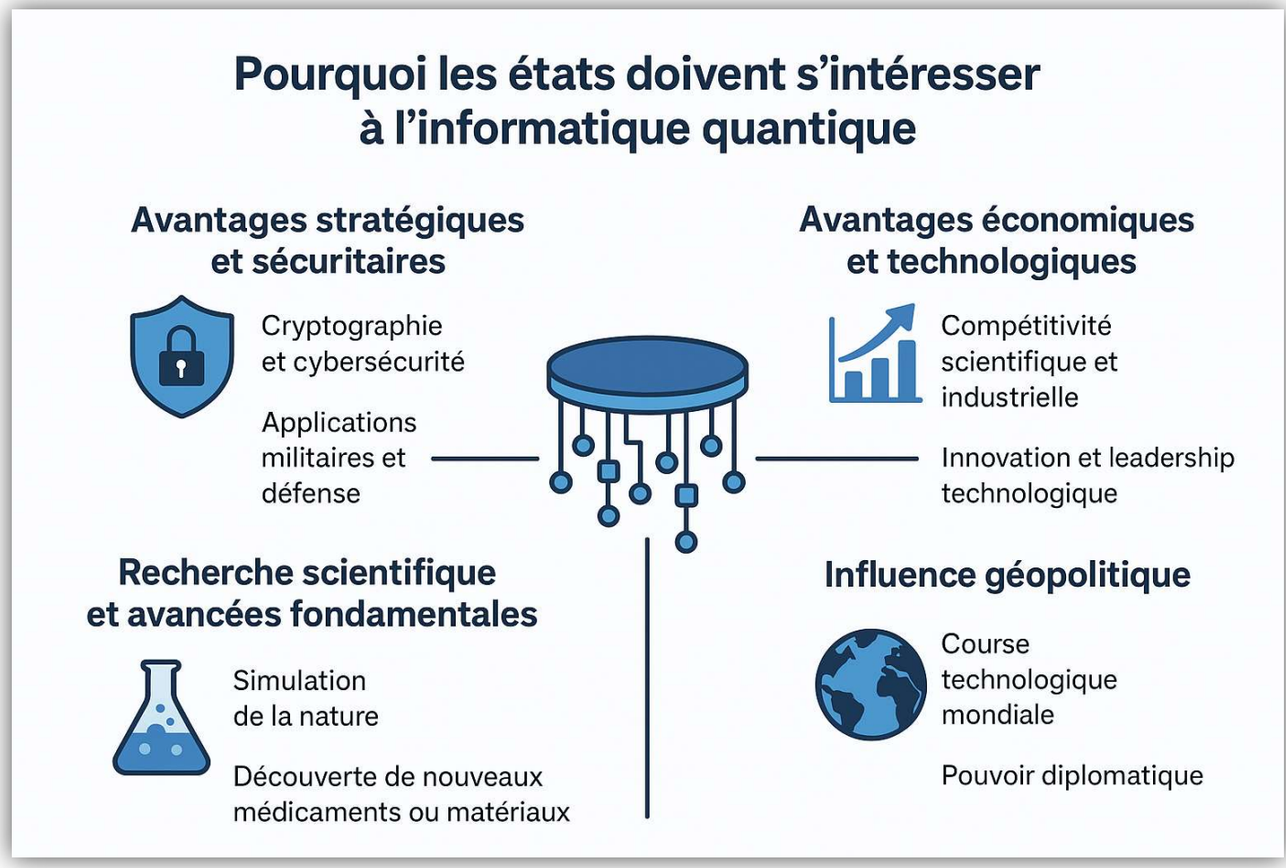
❑ **Pourquoi je m'en préoccupe ?**

Veille technologique + 20 ans de recherche en physique mathématique et rédaction d'une monographie en mécanique quantique avec un professeur de l'Université de Nagoya

❑ **Pourquoi les institutions doivent s'en préoccuper ?**

Les organismes de sécurité nationaux (NCSC aux UK, NIST aux USA,...) estiment que les ordinateurs quantiques pourraient être capables de casser des systèmes de cryptage actuels d'ici 2035. Mais il y a beaucoup plus :

illustration ChatGPT (septembre 2025)



Introduction

Qu'est-ce que l'informatique quantique ?

L'informatique quantique est une branche de l'informatique qui utilise les principes de la mécanique quantique pour encoder et traiter l'information.

Contrairement à l'informatique classique qui utilise des bits (0 ou 1), elle utilise des qubits régis par les lois de la mécanique quantique.

→ Permettra de résoudre certains problèmes hors de portée des ordinateurs classiques.

Principes fondamentaux

Un qubit («quantum bit») est l'unité d'information en informatique quantique. Il peut être dans les états $|0\rangle$, $|1\rangle$, ou dans une superposition

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

avec α et β des amplitudes complexes, $|\alpha|^2 + |\beta|^2 = 1$.

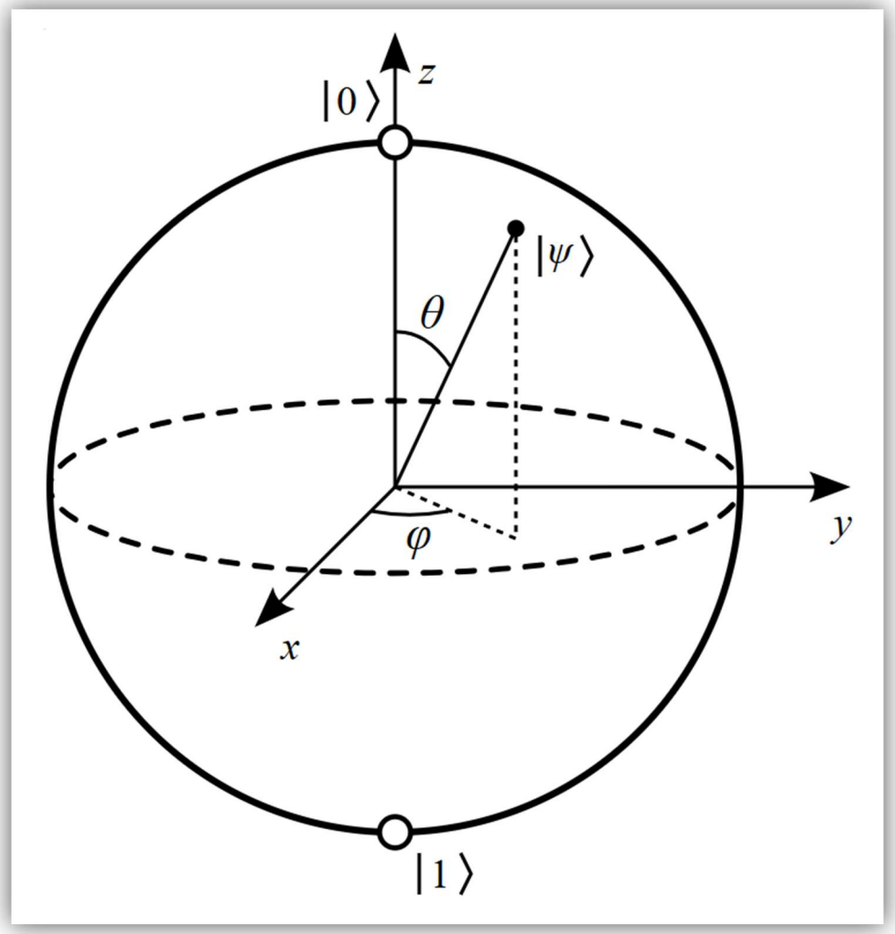
($|\psi\rangle$ peut être représenté comme un point d'une sphère de rayon 1 appelée «sphère de Bloch»)

Plusieurs approches pour fabriquer des qubits :

- ❑ Qubits supraconducteurs (Google, IBM, Rigetti, Intel)
- ❑ Ions piégés (IonQ, Quantinuum)
- ❑ Qubits à spin (Intel, Silicon Quantum Computing)
- ❑ Qubits photoniques (Xanadu)

Pas encore clair quelles technologies vont s'imposer…

sphère de Bloch (Wikipedia, septembre 2025)



Principes fondamentaux

Les principes de mécanique quantique utilisés en informatique quantique sont (entre autres) :

❑ Superposition et interférence des fonctions d'onde
(les qubits peuvent être en superposition de plusieurs états à la fois)

Par exemple : $\left(\frac{1}{2}|0\rangle + \frac{1}{4}|1\rangle\right) + \frac{1}{4}|0\rangle = \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$

❑ Intrication («entanglement») des fonctions d'onde
(les qubits peuvent être corrélés «instantanément», même à distance)

Par exemple : $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ (célèbre exemple appelé «Bell state»)

❑ Effondrement des fonctions d'onde lors d'une mesure
(l'état classique d'un système quantique est déterminé lors de sa mesure/observation 🐈)

Par exemple : $\frac{1}{2}|0\rangle + \sqrt{\frac{3}{4}}|1\rangle \longrightarrow$  $\longrightarrow |1\rangle$

Principes fondamentaux

Les portes logiques quantiques («quantum gates») sont l'équivalent des portes logiques classiques AND, OR, NOT,..., mais elles agissent sur des qubits plutôt que sur des bits.

Les portes quantiques...

- ❑ transforment l'état des qubits dans un circuit quantique
- ❑ réalisent des transformations réversibles (contrairement aux portes classiques qui peuvent être irréversibles)
- ❑ sont représentées mathématiquement par des matrices unitaires (ce qui garantit réversibilité + conservation de la norme des fonctions d'onde)

Principes fondamentaux

Les matrices unitaires proviennent de l'équation de Schrödinger en dimension finie...

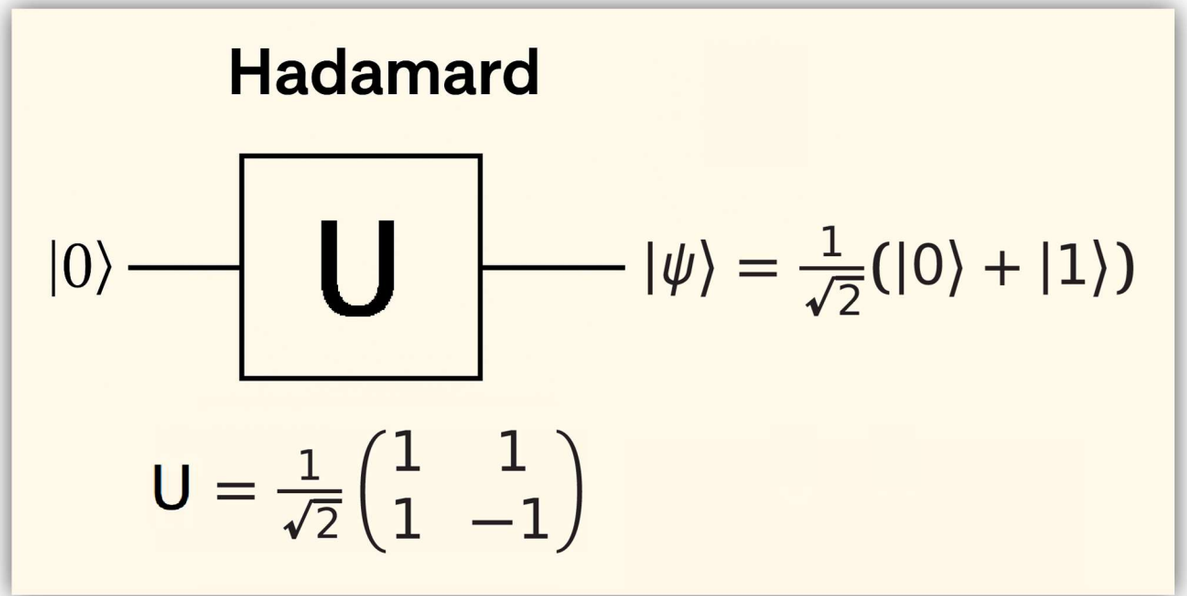
$$i\frac{\mathrm{d}}{\mathrm{dt}}|\psi(t)\rangle = H|\psi(t)\rangle \iff |\psi(t)\rangle = \mathrm{e}^{-itH}|\psi(0)\rangle \quad (H = \text{matrice hermitienne})$$

... et en temps discret $t = n$:

$$|\psi(n)\rangle = (\mathrm{e}^{-iH})^n|\psi(0)\rangle \iff |\psi(n)\rangle = U^n|\psi(0)\rangle \quad (U = \text{matrice unitaire})$$

Principes fondamentaux

Exemple de porte quantique :

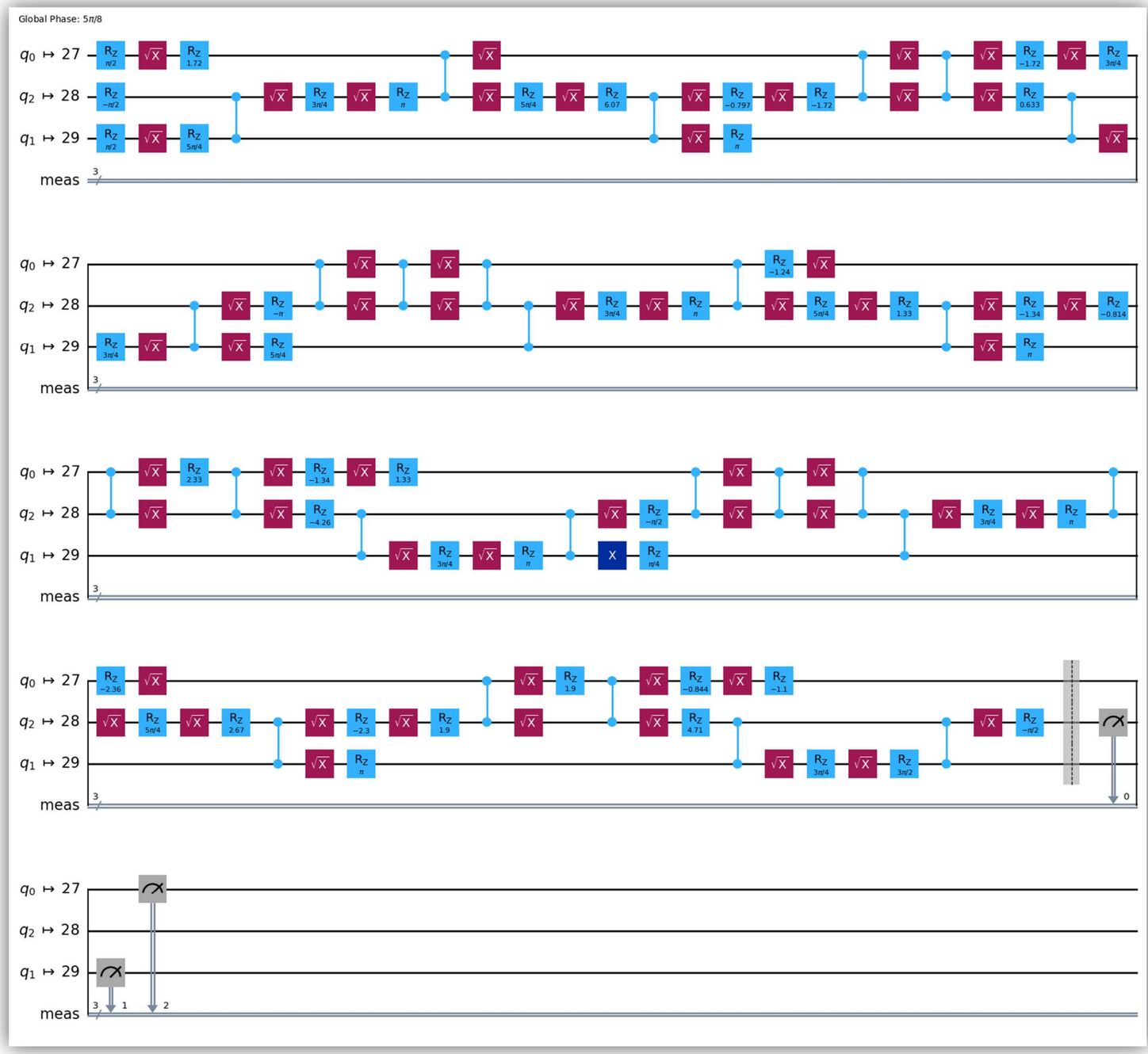


Principes fondamentaux

Exemple de circuit à 3 qubits exécuté sur l'ordinateur quantique «ibm_sherbrooke» le 7 mai 2025.

Programmation et diagramme réalisés avec la librairie Python open-source Qiskit introduite par IBM Research en 2017.

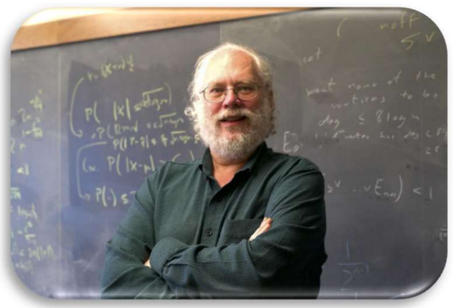
(diagramme à lire comme une partition de musique...)



Applications

Deux algorithmes emblématiques illustrent risques et opportunités offerts par l'informatique quantique.

CERN (mars 2021)



❑ **Algorithme de Shor («risque») :**
Permet (avec un ordinateur quantique abouti) la factorisation de grands nombres en un temps exponentiellement plus petit qu'avec les ordinateurs classiques.

➜ Permettra de casser divers protocoles de cryptage à clé publique tels que RSA, Diffie-Hellman, courbes elliptiques, etc.

dotquantum.io (date inconnue)

❑ **Algorithme de Grover («opportunité») :**
Permet (avec un ordinateur quantique abouti) la recherche d'un élément dans une liste non ordonnée en un temps quadratiquement plus petit qu'avec les ordinateurs classiques.

➜ Améliorera la rapidité de multiples applications industrielles basées sur la recherche d'un élément/configuration optimale dans un grand ensemble.

(le circuit antérieur implémente l'algorithme de Grover pour une liste de $2^3 = 8$ éléments 😀)

Applications

Les domaines d'applications de l'informatique quantique sont nombreux, à des étapes de développement plus ou moins avancé (recherche académique, PoC, ou déjà déployé) :

- ❑ Cryptographie et cybersécurité
- ❑ Optimisation et recherche opérationnelle
- ❑ Simulation de systèmes physiques et chimiques
- ❑ IA et Machine Learning
- ❑ Science des données et recherche d'information
- ❑ Communication quantique
- ❑ Métrologie et capteurs quantiques
- ❑ Finance et économie

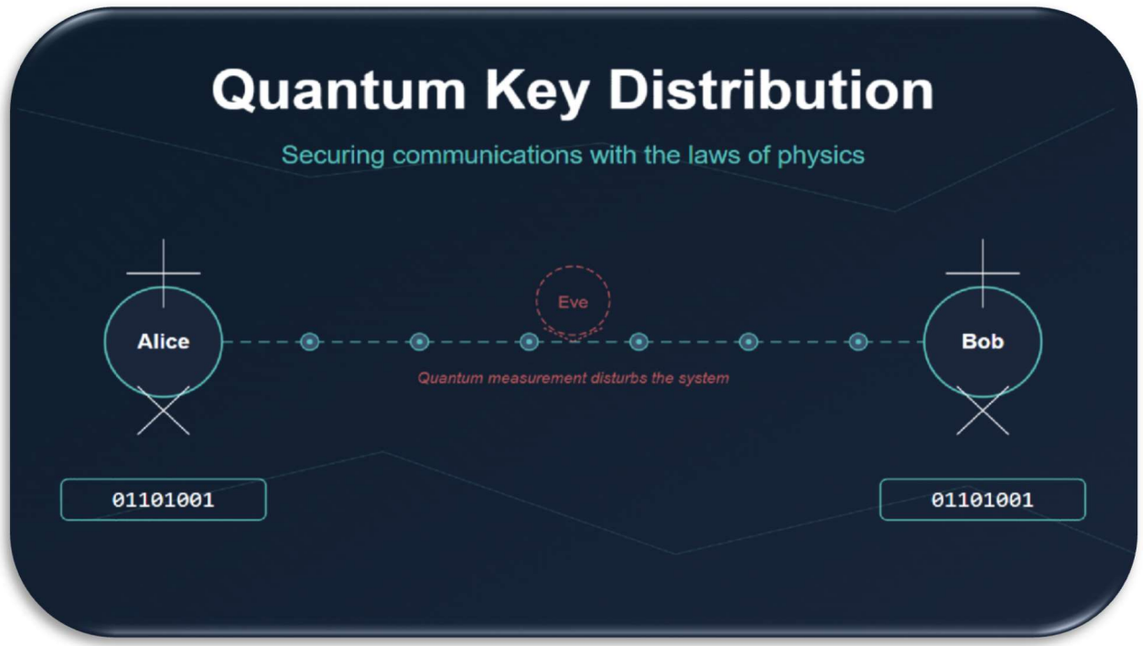


illustration Pranav Sanghadia (avril 2025)

(testé par la Chancellerie pour le vote électronique entre 2007 et 2014)

Limites et défis actuels

L'informatique quantique est encore dans sa phase NISQ («Noisy Intermediate-Scale Quantum» Computing). Les principaux défis sont :

- ❑ Amélioration de la stabilité (temps de cohérence), fiabilité et nombre de qubits
- ❑ Méthodes de correction des erreurs plus abordables (coût et infrastructure)
- ❑ Découverte de plus nombreux algorithmes quantiques utiles

Les progrès sont rapides mais il faudra des années (ou décennies) pour développer des ordinateurs quantiques «fault-tolerant» capables de résoudre des problèmes hors de portée des ordinateurs classiques.

Quelques actions déjà menées (non public)

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

OCSIN

Rafael Tiedra

Références

Informatique quantique :

https://en.wikipedia.org/wiki/Qubit

https://quantum.cloud.ibm.com/learning/en/courses/basics-of-quantum-information

https://quantum.cloud.ibm.com/learning/en/courses/fundamentals-of-quantum-algorithms

https://quantum.cloud.ibm.com/learning/en/courses/quantum-machine-learning/introduction

https://en.wikipedia.org/wiki/Introduction_to_Quantum_Mechanics_(book) (pour les enthousiastes)

Cryptographie post-quantique :

https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

https://quantum.cloud.ibm.com/learning/en/courses/quantum-safe-cryptography

https://www.coursera.org/learn/advanced-data-structures-rsa-and-quantum-algorithms

Librairies Python :

https://pennylane.ai/

https://en.wikipedia.org/wiki/Qiskit