

L'Informatique Quantique

Najah NAFFAH

Quantum Blockchain Secure

22 Mai, 2023

Références – Pour comprendre davantage et aller plus loin dans l'exploration ... !

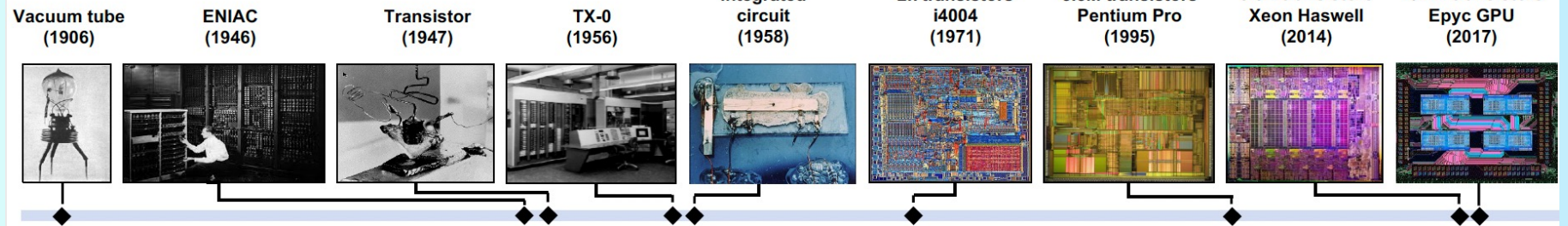
- <https://www.college-de-france.fr/fr/chaire/frederic-magniez-informatique-et-sciences-numeriques-chaire-annuelle> cours de F. Magniez avec d'autres conférenciers (permet d'approfondir le sujet pour ceux qui sont tenaces)
- <http://exo7.emath.fr/cours/livre-quantum.pdf> (par Arnaud Bodin avec des vidéos sur YouTube accessibles en cliquant sur les liens au début de chaque chapitre)
- <https://arxiv.org/pdf/1804.03719.pdf> Quantum Algorithm Implementations for Beginners – Panorama de tous les algos en cours de développement
- <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-decade> Brochure d'IBM - excellente initialisation sur les applications, perspectives, et challenges du Quantique

Sommaire

- Vue Globale du Domaine – (parcours, applications, modèles, marché)
- Mécanique Quantique – les pionniers et les postulats
- Naissance de l'idée de l'Ordinateur Quantique (OQ)
- Les Systèmes Quantiques – concepts de base
- Les 1^{ers} protocoles:
 - Inégalités de Bell
 - Téléportation, codage super-dense
 - Distribution quantique de clefs (BB84)
- Les premiers algorithmes – l'approche quantique, les preuves de l'avantage quantique, les applications utiles (Shor, Grover)
- La nouvelle génération d'algorithmes
- Retour à l'Ordinateur Quantique – les modèles physiques – avantages et inconvénients
- Analyse des offres - la concurrence
- Les enjeux, les plans nationaux et la course au Leadership
- Conclusions et perspectives

IT Classique et Quantum Computing: Les Dates Clefs

Classical Computing (Electronic)

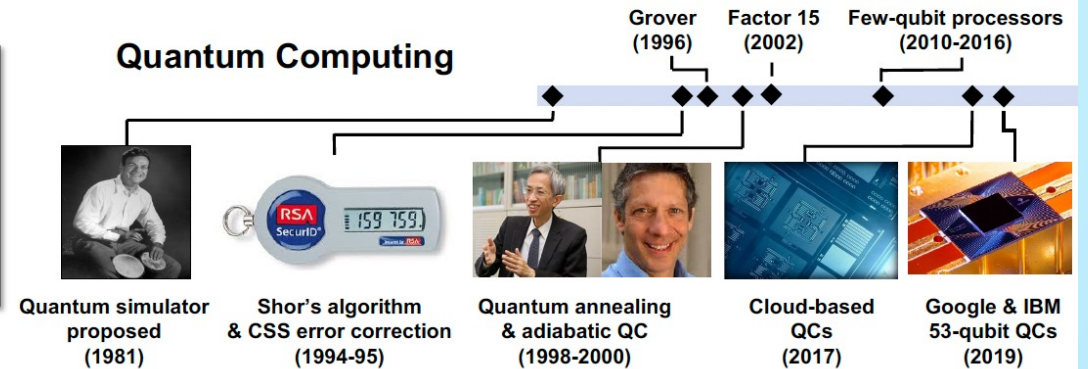


Quantum computing is transitioning from scientific curiosity to technical reality.

Advancing from discovery to useful machines takes time & engineering

You must be in the game to play

Quantum Computing



IBM 433 up to 1121 in 2023
D Wave 2000 - 5000
Pasqal 100 and going up

Les Marchés

Les Capteurs

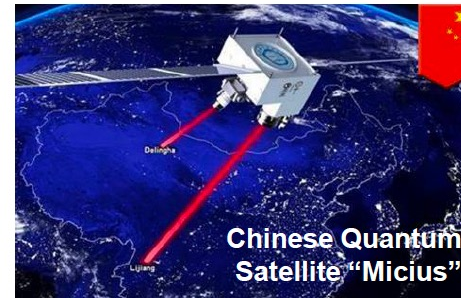
Quantum Sensing



Improves sensitivity, drift, & spatial resolution

Les Réseaux

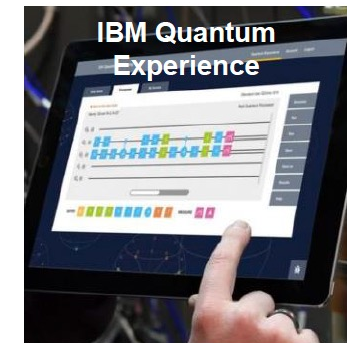
Quantum Networks



Enables distributed quantum states

L'Informatique

Quantum Computing



Solves select problems that are intractable with classical computing

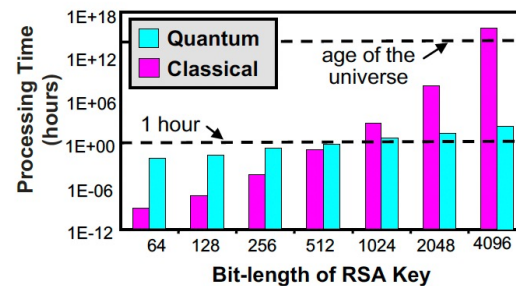
Quantum Information Science utilizes a quantum mechanical description of nature to sense, communicate, and process/compute information in ways unobtainable by means based on a classical description of nature

22/05/2023

Les Modèles de Quantum Computing et les Applications Cibles

Universal, Fault-Tolerant Quantum Computer

Shor's Algorithm for Prime Factorization:
RSA Key Decryption



Gate-Based Applications:

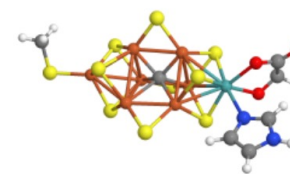
- RSA key decryption
- Database searching
- Linear equation sampling

Quantum speed-up exists
over known classical algorithms

Digital & Analog Quantum Simulator

Simulation of Reaction Mechanisms:
Biological Nitrogen Fixation to Produce Ammonia

FeMo Cofactor in Nitrogenase Protein



PNAS 114, 7555-7560 (2017); arXiv:1605.03590

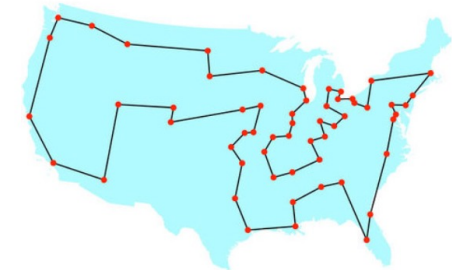
Simulation Applications:

- Quantum chemistry
- Drug development
- Materials science

Quantum speed-up exists
over known classical algorithms

Quantum Annealer

Route Optimization:
Traveling Salesman Problem

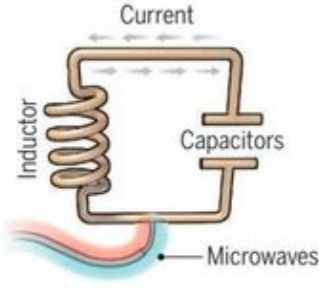
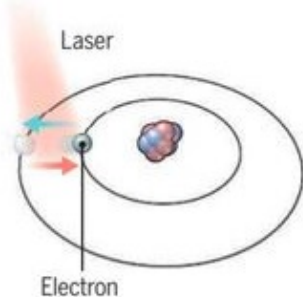
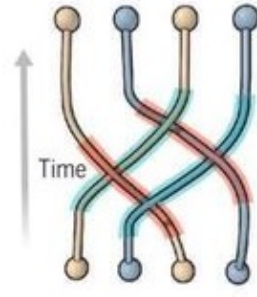
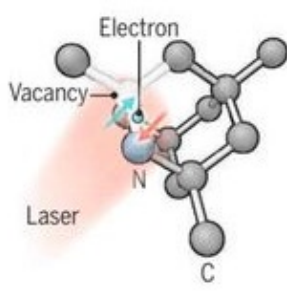


Annealing Applications:

- Supply transport optimization
- Sensor & satellite tasking
- Pattern recognition

Unknown if quantum speed-up exists
over known classical algorithms

Comparaison des Technos

				
Superconducting loops	Trapped ions	Silicon quantum dots	Topological qubits	Diamond vacancies
Company support Google, IBM, Quantum Circuits	ionQ	Intel	Microsoft, Bell Labs	Quantum Diamond Technologies
Pros Fast working. Build on existing semiconductor industry.	Very stable. Highest achieved gate fidelities.	Stable. Build on existing semiconductor industry.	Greatly reduce errors.	Can operate at room temperature.
Cons Collapse easily and must be kept cold.	Slow operation. Many lasers are needed.	Only a few entangled. Must be kept cold.	Existence not yet confirmed.	Difficult to entangle.

La Mécanique Quantique

Quantum Mechanics

- La théorie de la mécanique quantique est une description mathématique du monde à très petite échelle et constitue la théorie la plus précise pour comprendre et prédire les propriétés de l'univers physique.
- *Les interactions quantiques sont différentes de celles que nous vivons au quotidien*

Quantum Mechanics in a Nutshell

1. States

Every physical system has a state space which is a complex vector space. An isolated system's state can be described by a unit vector in that state space.

$$|\psi\rangle \in \mathbb{C}^n$$

2. Dynamics

An isolated quantum system's evolution is described by a unitary matrix acting on the system's state space.

$$|\psi'\rangle = U|\psi\rangle$$

3. Measurement

Measurement operators describe how we get information out of a quantum system.

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

$$|\psi_m\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$$

$$\sum_m M_m^\dagger M_m = I$$

4. Combining systems

Quantum state spaces combine via tensor products.

state space A

state space B

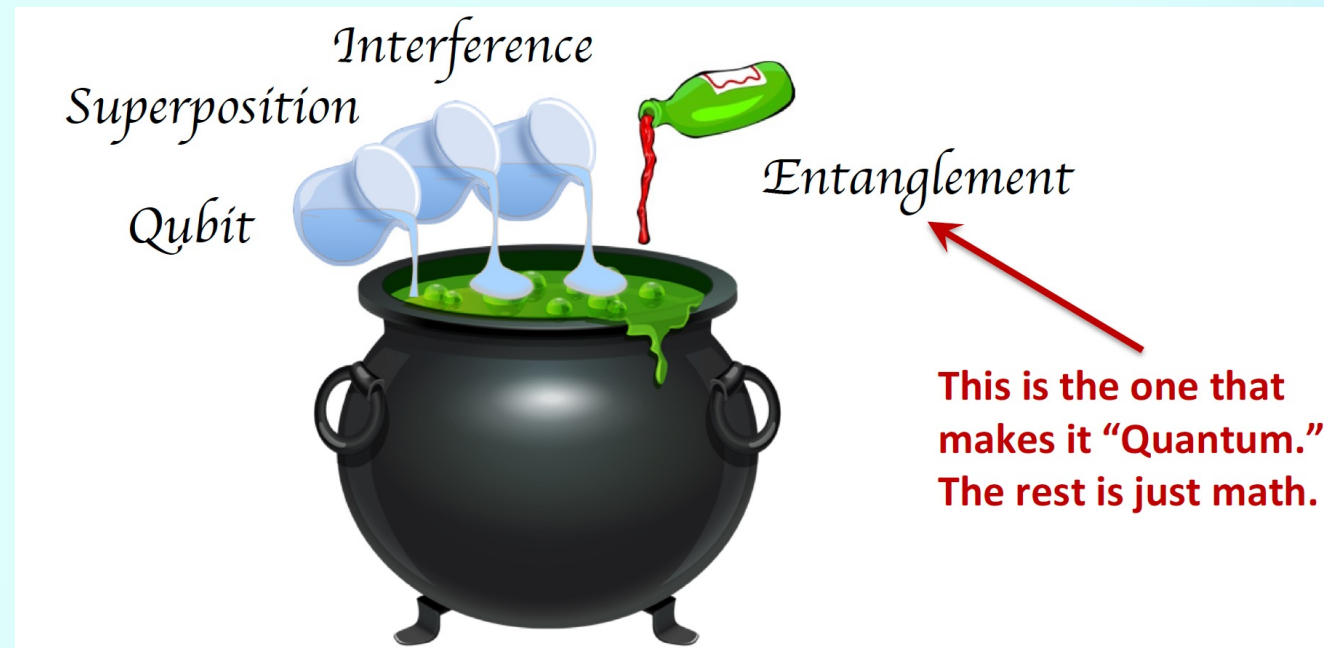
$\Rightarrow$

combined state space $A \otimes B$

quantum.country/qm

La Mécanique Quantique dans le cadre de l'Informatique Quantique:

les propriétés à exploiter pour résoudre des problèmes **spécifiques**



- 100 qubits = 2^{100} states
- 2^n complex coefficients describe the state of a composite quantum system with n qubits
- Quickly reaches number of particles in the universe

Qu'est ce qu'un ordinateur quantique

- ▶ L'ordinateur quantique est un ordinateur qui exploite les propriétés de la matière (particules) telles que *superposition*, *intrication*, et *interférence*, décrites par la Mécanique Quantique, pour faire des calculs spécifiques qui ne sont pas à la portée des ordinateurs classiques
- ▶ Les Fondations sur 3 domaines:



Mécanique Quantique



Théorie de
l'information Quantique

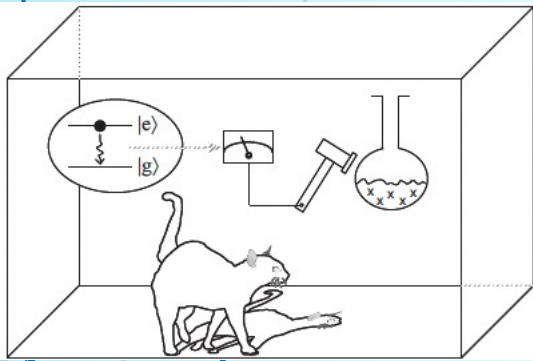


L'informatique
(Computer Science)

La Superposition

La Superposition –
sera définie formellement avec l'introduction du Qubit

Schrödinger's Cat: Dead or Alive



You can only MEASURE either dead or alive, not both

John Bell – Exploitation de l'Intrication

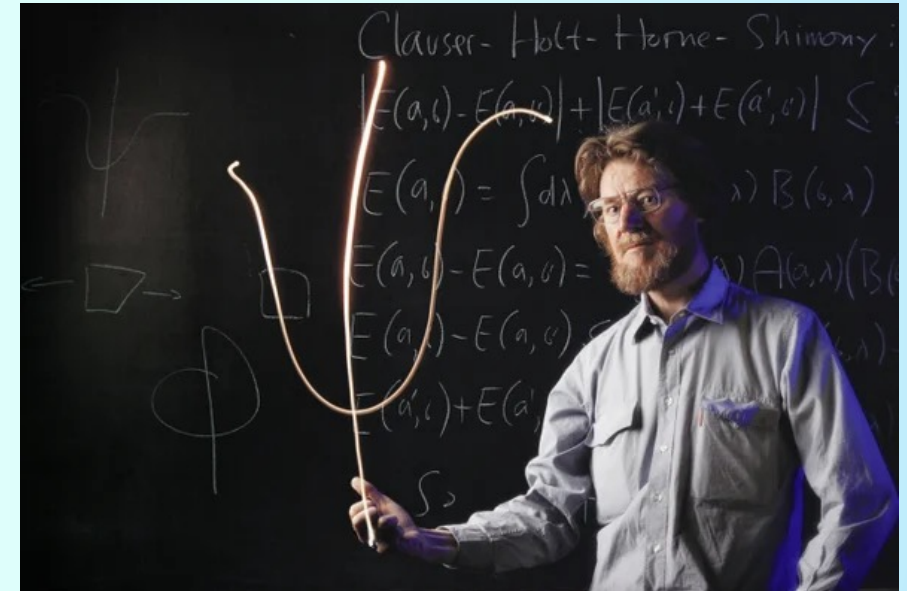
l'Intrication

Le théorème de Bell est l'héritage le plus célèbre de John Bell.

Ce théorème a tracé une ligne de démarcation entre la mécanique quantique (MQ) et le monde tel que nous le connaissons d'une façon intuitive.

Dans sa forme la plus simple, le théorème de Bell s'énonce comme suit :

“Aucune théorie physique de variables cachées locales (Local Hidden Variables) ne peut jamais reproduire toutes les prédictions de la mécanique quantique”



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

No physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics

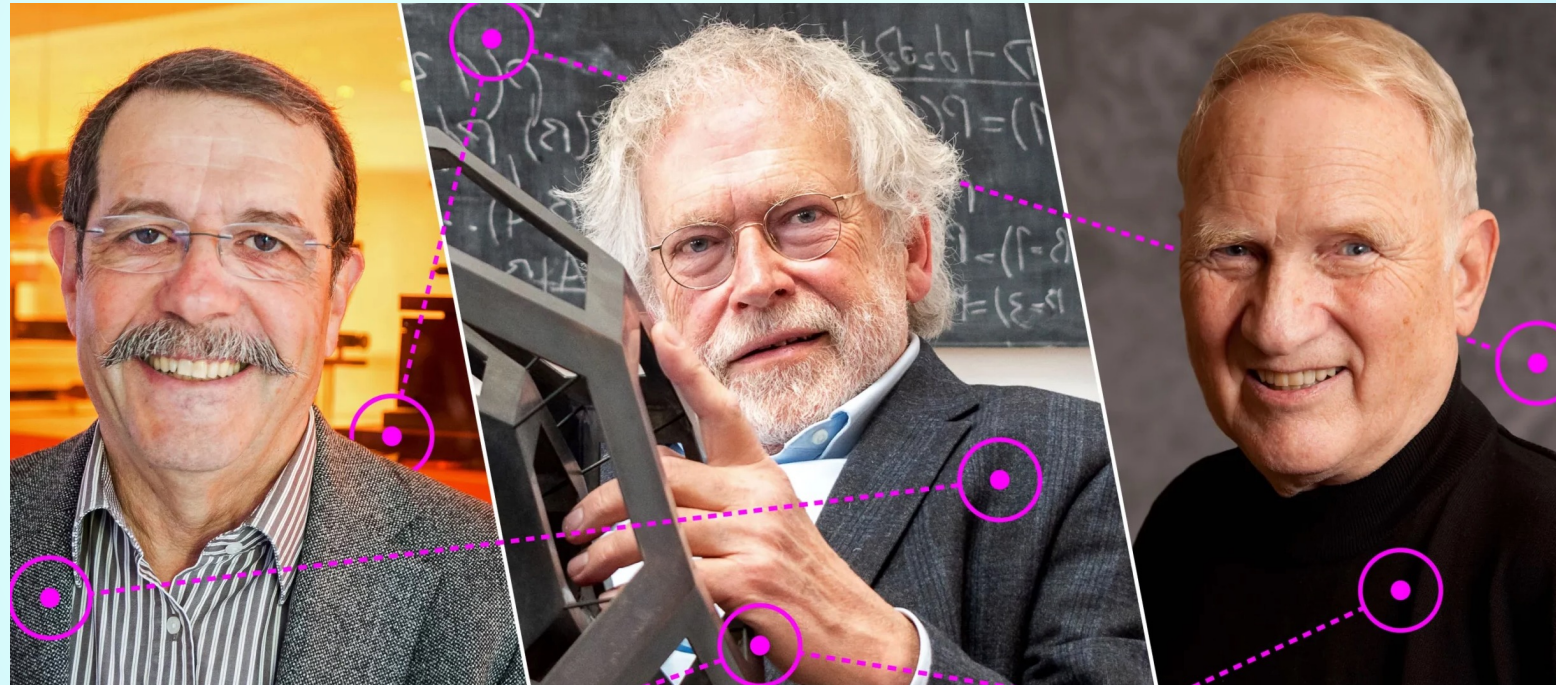
22/05/2023

Dans le sillage de John Bell

Ceux qui ont fait les expérimentations

Pioneering Quantum Physicists Win Nobel Prize in Physics

l'Intrication



Alain Aspect, Anton Zeilinger, John Clauser have won the 2022 Nobel Prize in Physics for groundbreaking experiments with entangled particles.

22/05/2023

Qu'est ce qu'un Qubit ?

Un Bit Classique peut prendre deux valeurs différentes discrètes (0 ou 1).

Un Qubit peut prendre une infinité de valeurs en continue

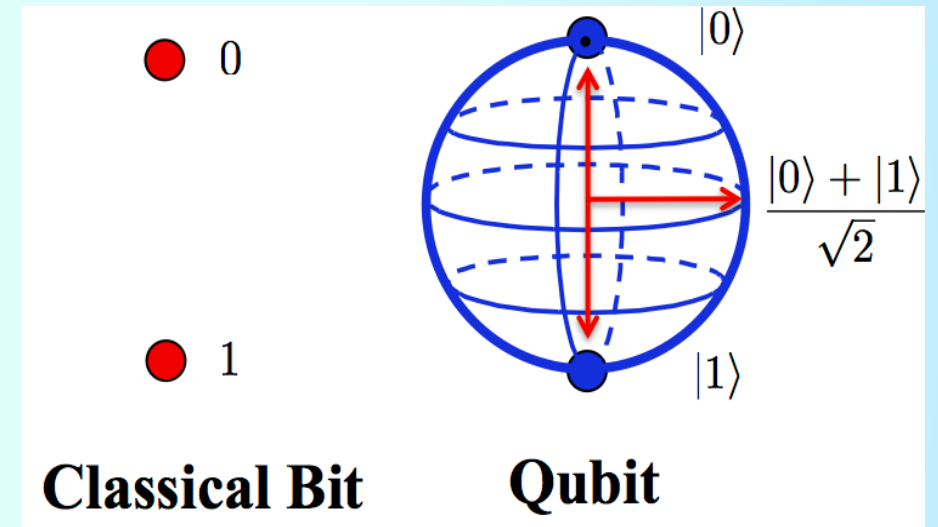
Les Qubits vivent dans un espace vectoriel, celui de *Hilbert*, avec des états de base qui sont: $|0\rangle$ and $|1\rangle$

Un Qubit générique $|\Psi\rangle$ en mode superposition s'écrit :

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

Où α et β sont des nombres complexes, appelés Amplitudes avec:

$$|\alpha|^2 + |\beta|^2 = 1$$



Rappel – Notations Dirac

1 Qubit

$$|0\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \leftrightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

2 Qubits

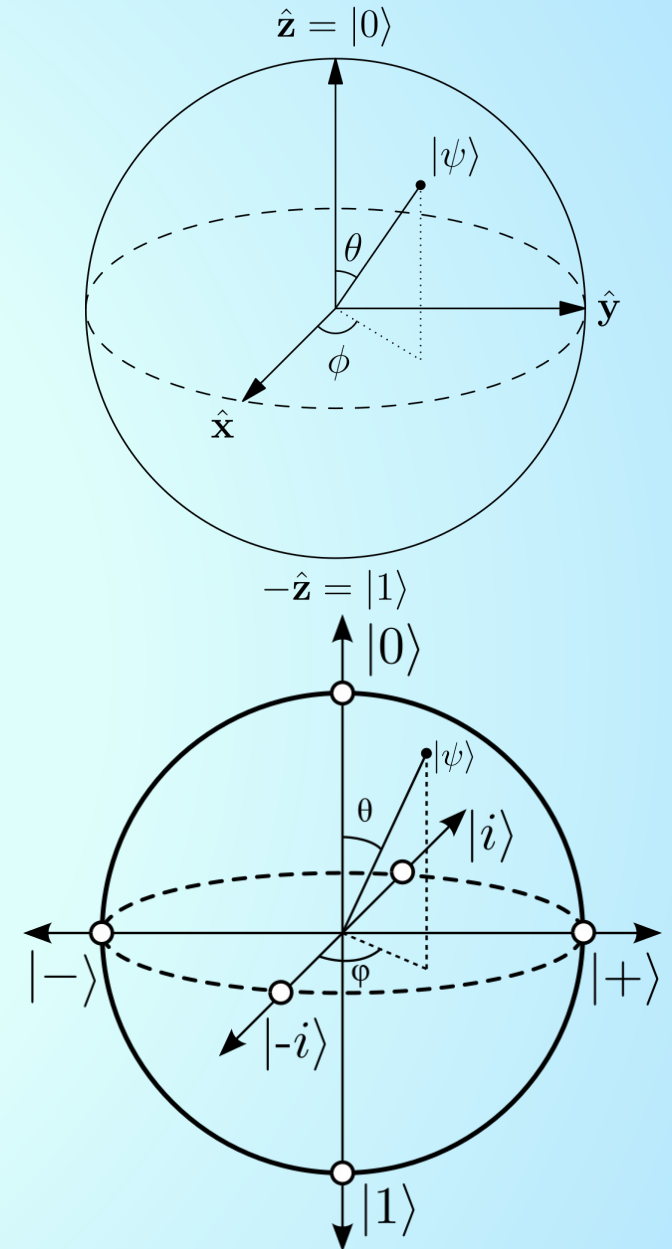
$$|00\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle \leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle \leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

2 Qubits

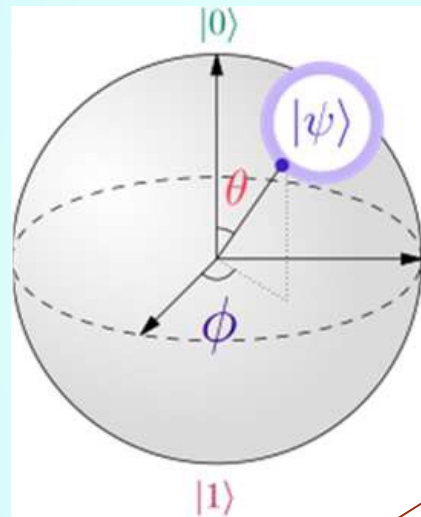
- Si on avait deux bits classiques, on aurait 4 états: 00, 01, 10, 11
- Un système à 2-Qubits aura 4 états de Base (Computational Basis States CBS) que l'on note: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$
- Une paire de Qubits, peut aussi exister en mode superposition.
- La description de l'état du système est alors $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
- Aux États de base (CBS) sont associés des coefficients complexes appelés amplitudes
- La condition de sommations des probabilités à 1 (Normalisation) est toujours respectée: $\sum_{x \in \{0,1\}^2} |\alpha_x|^2 = 1$
- La mesure du 1^{er} Qubit donne 0 avec une probabilité de $|\alpha_{00}|^2 + |\alpha_{01}|^2$

Le Qubit sur la Sphère de Bloch

- Tous les états dans lesquels le qubit pourrait se trouver sont représentés par des points sur une sphère unitaire unitaire appelée Sphère de Bloch
- $|0\rangle$ se trouve au pôle nord et $|1\rangle$ au pôle sud.
- Les points sur la sphère correspondent à des **états quantiques**.
- A propos de la superposition, mathématiquement, le qubit est toujours en superposition parce que son état peut se trouver aux pôles $|0\rangle$ ou $|1\rangle$ ou à n'importe quel point entre les deux.



Coordonnées Polaires d'un Qubit



$$\left. \begin{array}{l} \text{Diagram of Bloch sphere with state } |\psi\rangle \text{ and angles } \theta \text{ and } \phi \end{array} \right\} \begin{aligned} |\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\ &= e^{i\gamma} \left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \right) \\ &0 \leq \theta \leq \pi, \quad 0 \leq \phi \leq 2\pi \end{aligned}$$

Global Phase

Relative Phase

Résumé – Qubit, Visualisation, Action

- La plus petite unité d'information quantique est le qubit.
- Le qubit possède deux états orthogonaux : $|0\rangle$ et $|1\rangle$.
- Un qubit peut être une **superposition** de ces états avec des **amplitudes complexes**.
- La norme carrée des amplitudes donne la probabilité de mesurer le qubit comme un "0" ou un "1", et selon le résultat, le qubit s'effondre en $|0\rangle$ ou $|1\rangle$.
- Les qubits peuvent également être **mesurés dans d'autres bases orthonormées**.
- Un qubit peut être visualisé sur la **sphère de Bloch**.
- Les qubits sont manipulés par des **portes quantiques**,
- Une **porte** à qubit unique est une rotation sur la sphère de Bloch.
- Un **circuit quantique** est un dessin représentant les portes quantiques qui agissent sur un qubit,

Ligne Quantique, Mesure, Portes

L'output (résultat) peut être représenté par un histogramme de la distribution de probabilité.

Il est important de rappeler que alpha et beta: $\alpha|0\rangle + \beta|1\rangle$ sont des amplitudes de l'état et sont des nombres complexes.

D'autre part, les valeurs $|\alpha|^2$ and $|\beta|^2$ sont des nombres réels positifs dans l'intervalle $[0 ; 1]$ et sont appelées probabilités

$$|\psi\rangle \longrightarrow \boxed{\text{Measurement}} = 0 \text{ or } 1$$

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{\text{Measurement}} = \begin{cases} 0, & \text{with probability } |\alpha|^2, \\ 1, & \text{with probability } |\beta|^2. \end{cases}$$

$$|0\rangle \longrightarrow \boxed{H} \longrightarrow |+\rangle.$$

$$|0\rangle \longrightarrow \boxed{H} \longrightarrow \boxed{\text{Measurement}} = \begin{cases} 0, & \text{with probability } \frac{1}{2}, \\ 1, & \text{with probability } \frac{1}{2}. \end{cases}$$

Porte Quantique

- Une porte quantique est la transformation $|\psi\rangle \mapsto A|\psi\rangle$ où A est une matrice unitaire.

$$|\psi\rangle \longrightarrow \boxed{A} \longrightarrow A|\psi\rangle$$

- Si l'entrée $|\psi\rangle$ est un n -qubit, alors A une matrice de taille 2^n , la sortie est un n -qubit.
- Comme la matrice A est unitaire alors en particulier la transformation est inversible. C'est une différence majeure par rapport à une porte de l'informatique classique (par exemple une porte AND n'est pas inversible).
- Une matrice unitaire A : $A^*A=I$ et $A^{-1}=A^*$

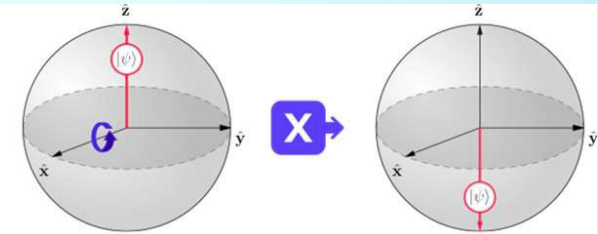
Les Portes de Pauli (agissant sur un Qubit)

1

Pauli-X (bit-flip)

Equivalent d'une porte **NOT**. Rotation de π autour de l'axe X.

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

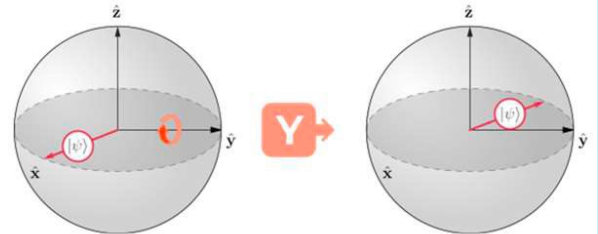


2

Pauli-Y

Rotation de π autour de l'axe Y de la sphère de Bloch.

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

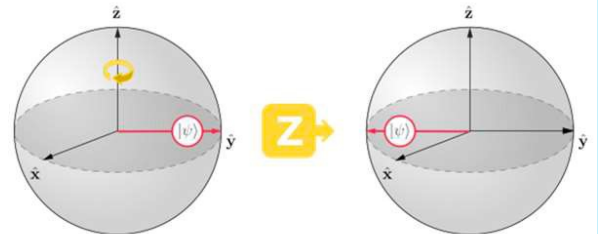


3

Pauli-Z (phase-flip)

Rotation de π autour de l'axe Z (changement de phase).

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



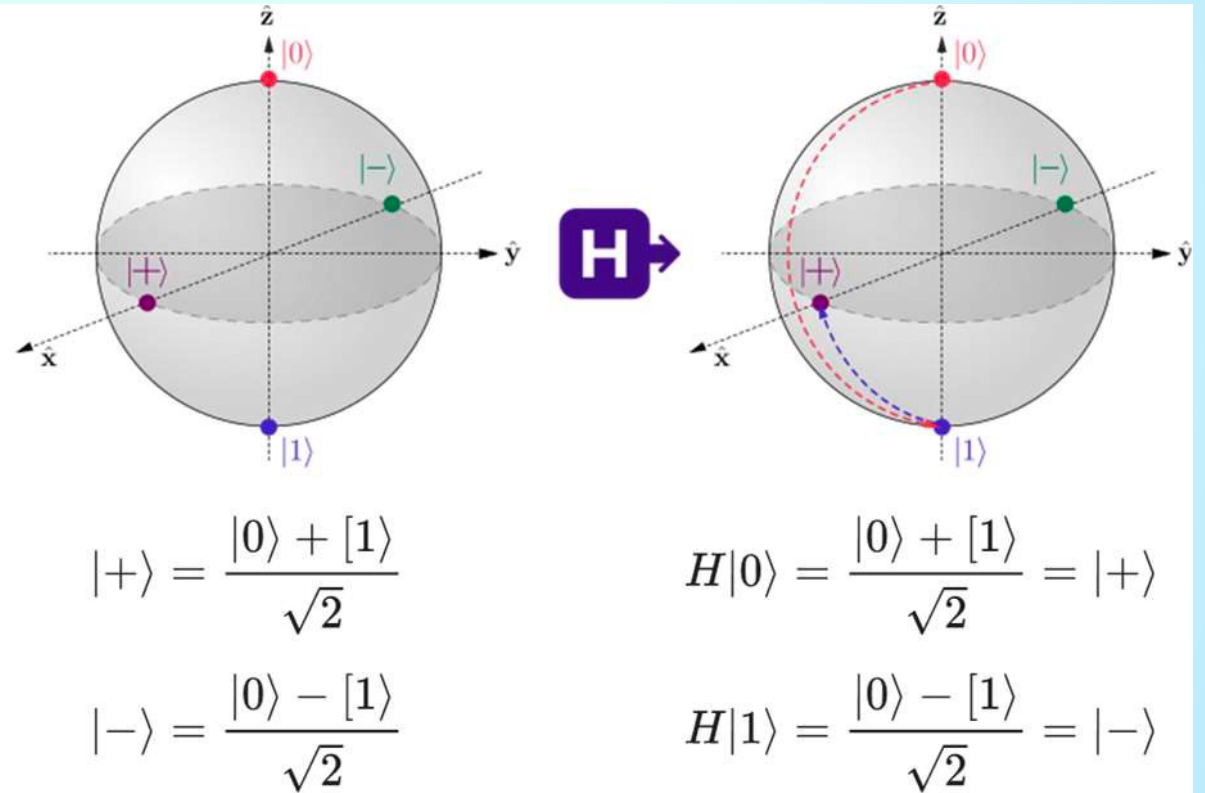
Porte Hadamard

(mettre les qubits en superposition)

Hadamard

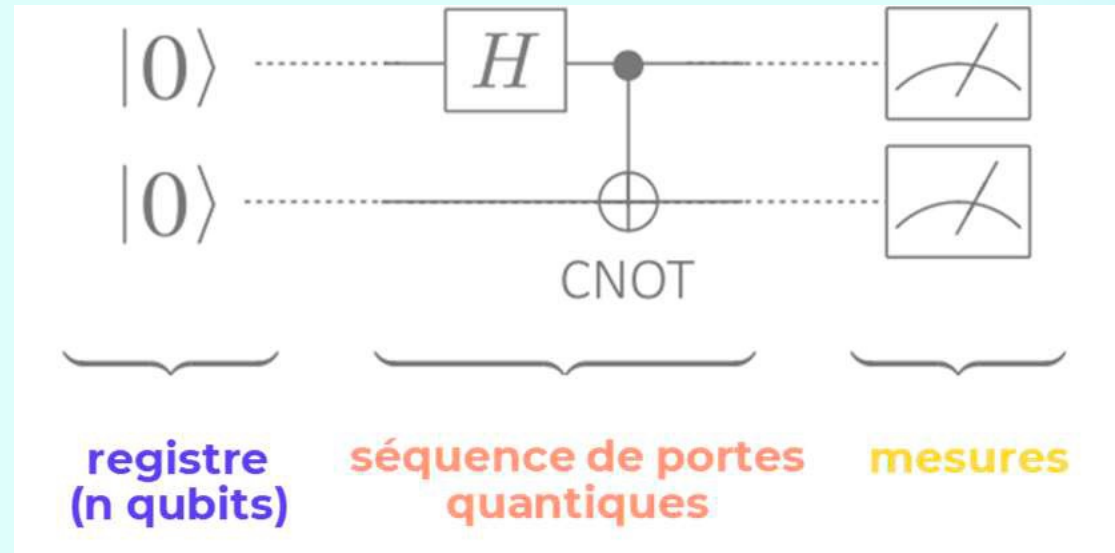
Combinaison de deux rotations: π sur l'axe des X, suivie par $\pi / 2$ sur l'axe des ordonnées.

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



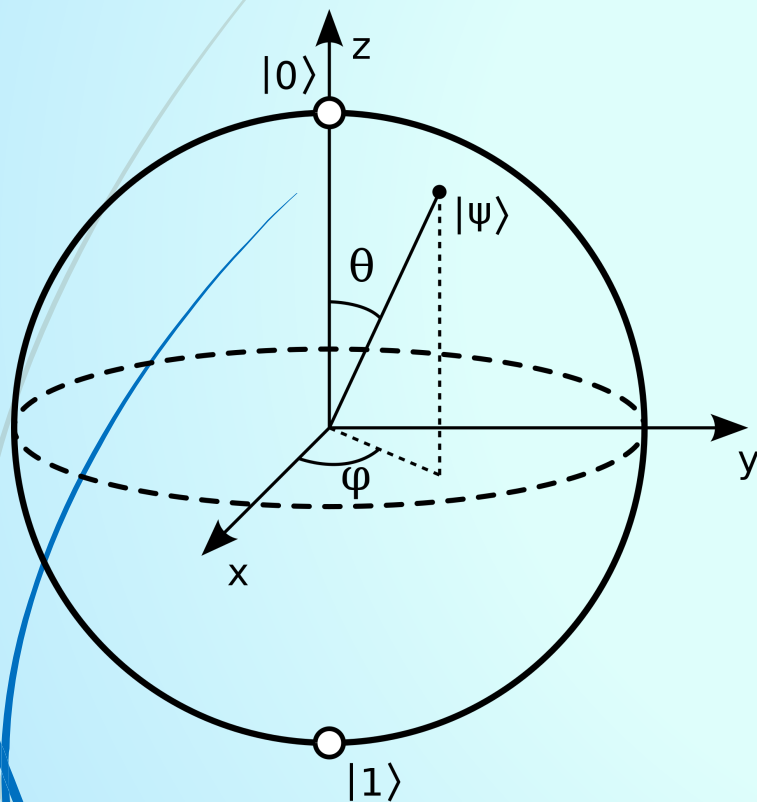
Circuit Quantique

(Registre entrées, Transformations, Mesures)



Résumé

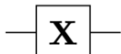
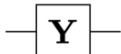
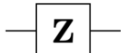
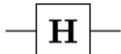
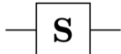
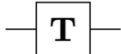
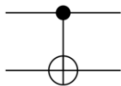
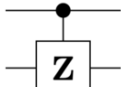
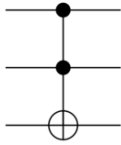
Les Portes agissant sur 1, 2, 3 Qubits



1 Qubit

2 Qubits

3 Qubits

Operator	Gate(s)		Matrix
Pauli-X (X)			$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)			$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)			$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)			$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)			$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)			$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

L'effet de 2 portes Hadamard



1 Hadamard

$$H |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

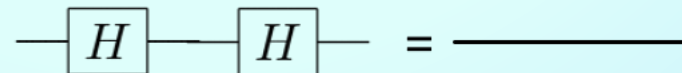
$$H |1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

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

2 Hadamard

$$H H |0\rangle = \frac{1}{\sqrt{2}} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |0\rangle$$

$$H H |1\rangle = \frac{1}{\sqrt{2}} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} - \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |1\rangle$$



La Porte Controlled-NOT

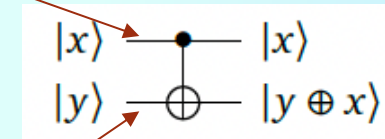
Si le bit de contrôle est $|0\rangle$, le bit cible est inchangé
 Si le bit de contrôle est $|1\rangle$ le bit cible subit une addition binaire (flip)

Toute porte quantique à n-qubits peut être réalisée de façon équivalente par un circuit ne comportant que des portes CNOT et des portes à 1-qubit

Porte permettant du *If-Then-Else*
 Essentielle pour l'intrication

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Bit de contrôle



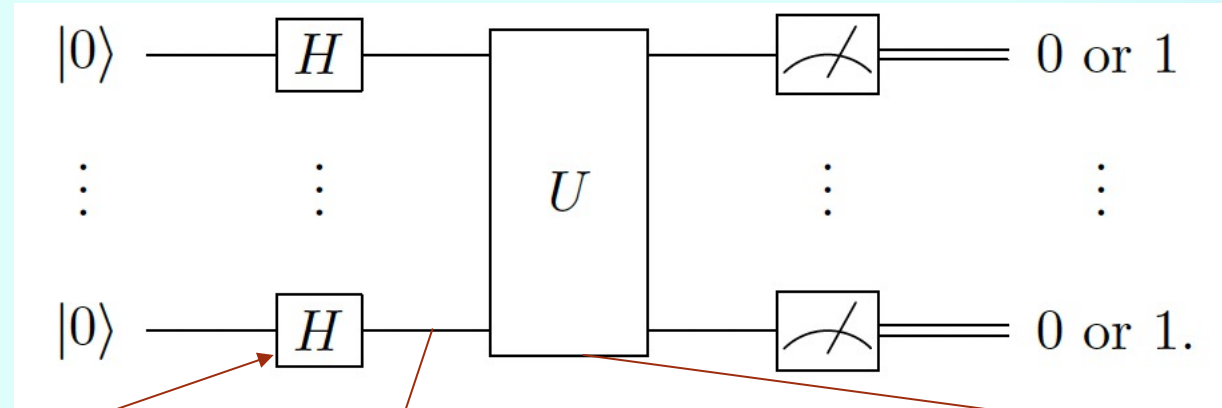
Bit cible

$$|0.0\rangle \xrightarrow{\text{CNOT}} |0.0\rangle \quad |0.1\rangle \xrightarrow{\text{CNOT}} |0.1\rangle \quad |1.0\rangle \xrightarrow{\text{CNOT}} |1.1\rangle \quad |1.1\rangle \xrightarrow{\text{CNOT}} |1.0\rangle$$

Système de “n” qubits

- Les systèmes quantiques sont généralement constitués de n-qubits
- Les états de base de calcul de ce système sont de la forme $|x_1 x_2 \dots x_n\rangle$
- Un état quantique d'un tel système est spécifié par 2^n amplitudes.
- Pour $n = 500$, ce nombre est supérieur au nombre estimé d'atomes dans l'univers !
- Impossible de stocker tous ces nombres complexes sur les ordinateurs classiques les plus puissants
- “Hilbert space is Huge space!”
- Cependant, la nature manipule de telles quantités de données, même pour des systèmes ne contenant que quelques centaines d'atomes.

Le Parallélisme Quantique



En appliquant
n portes Hadamard
Sur les Kets d'entrée
On transforme leurs
états en $|+\rangle$

$$(H|0\rangle) \otimes \dots \otimes (H|0\rangle)$$

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \otimes \dots \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right)$$

$$\frac{1}{\sqrt{2^n}} (|0 \dots 0\rangle + |0 \dots 01\rangle + |0 \dots 10\rangle + \dots + |1 \dots 1\rangle)$$

- U est appliqué simultanément sur tous les kets du registre d'entrée
- Il est possible d'effectuer 2^n calculs simultanés sur un n-qubits

Exemple d'un Circuit Quantique

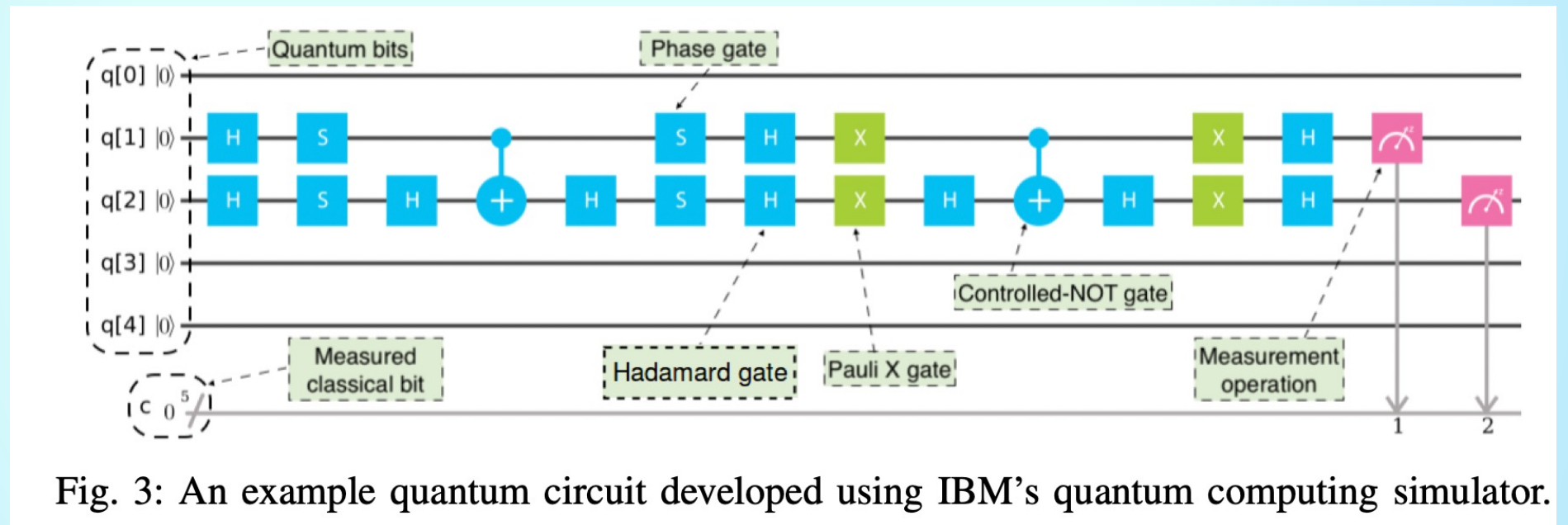
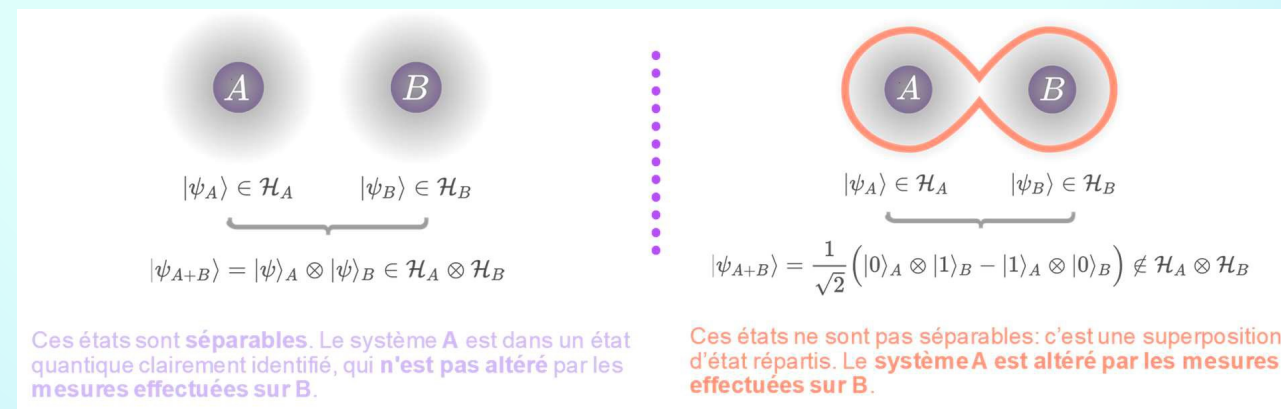


Fig. 3: An example quantum circuit developed using IBM's quantum computing simulator.

Intrication - Entanglement

- L'Intrication - L'intrication est une propriété spécifique de certains états de superposition multiparticules, où la mesure de l'état d'une particule fait s'effondrer l'état des autres particules, même si les particules sont éloignées les unes des autres sans possibilité apparente d'interaction.
- Cela se produit lorsque les fonctions d'onde des différentes particules ne sont pas séparables (en termes mathématiques, lorsque la fonction d'onde du système entier ne peut pas être écrite comme un produit des fonctions d'onde de chaque particule).
- Il n'existe pas d'analogie classique à ce phénomène



Bell states - Création des états de Bell à partir de deux portes ! (H, CNOT)

- ▶ Avec le circuit commençant par une porte **Hadamard** suivie par une porte **CNOT**, on transforme les 4 états de base selon le tableau ci-dessous:

In	Out
$ 00\rangle$	$(00\rangle + 11\rangle)/\sqrt{2} \equiv \beta_{00}\rangle$
$ 01\rangle$	$(01\rangle + 10\rangle)/\sqrt{2} \equiv \beta_{01}\rangle$
$ 10\rangle$	$(00\rangle - 11\rangle)/\sqrt{2} \equiv \beta_{10}\rangle$
$ 11\rangle$	$(01\rangle - 10\rangle)/\sqrt{2} \equiv \beta_{11}\rangle$

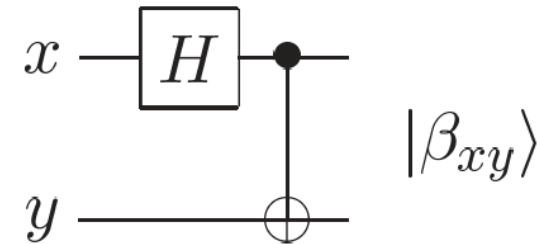
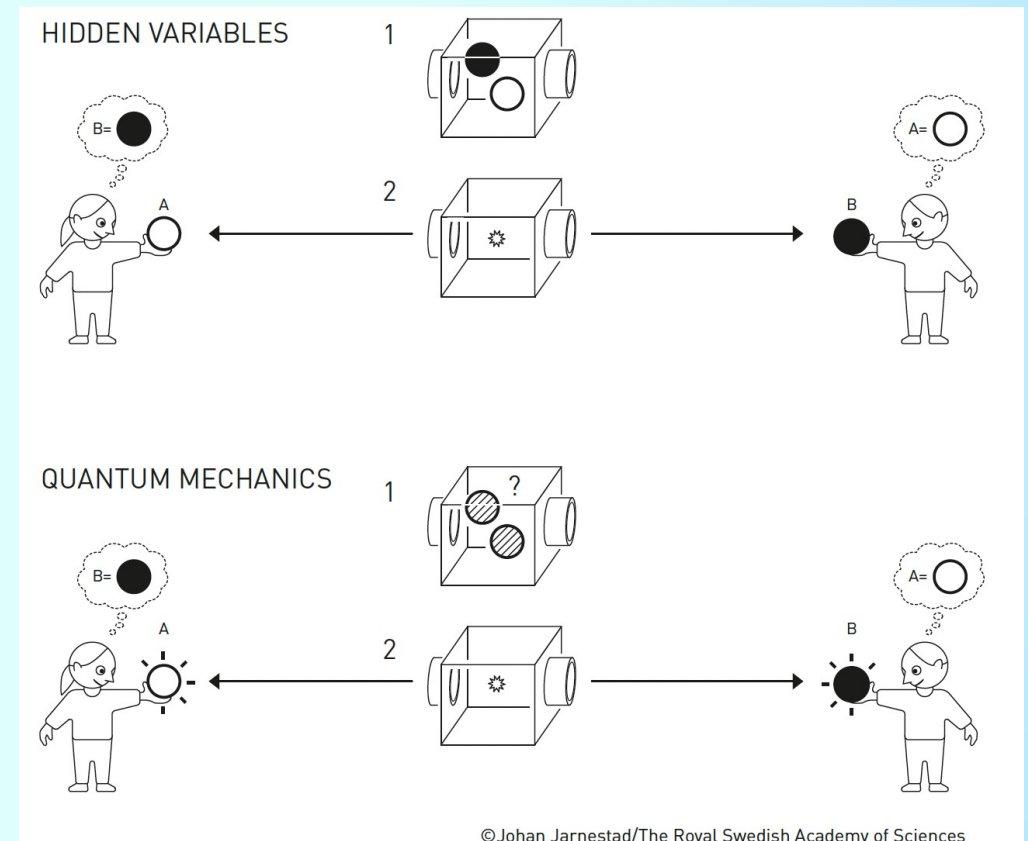


Figure 1.12. Quantum circuit to create Bell states, and its input–output quantum ‘truth table’.

Entangled Pairs

Est ce que la Couleur existe, lorsque personne ne regarde ?

- Les paires intriquées de la mécanique quantique peuvent être comparées à une **machine qui lance des balles de couleurs opposées dans des directions opposées**.
- Lorsque Bob attrape une boule et voit qu'elle est **noire**, il sait immédiatement qu'Alice a attrapé une boule **blanche**.
- Dans une théorie qui utilise des **variables cachées**, les boules ont toujours contenu une information cachée (hidden variables) sur la couleur à montrer.
- Cependant, la **mécanique quantique** indique que les boules **étaient grises** jusqu'à ce que quelqu'un les regarde, l'une devenant alors aléatoirement blanche et l'autre noire.
- Les inégalités de Bell montrent qu'il existe des expériences qui peuvent illustrer la différence entre ces deux cas.
- Ces expériences ont prouvé que la description **de la mécanique quantique est correcte**



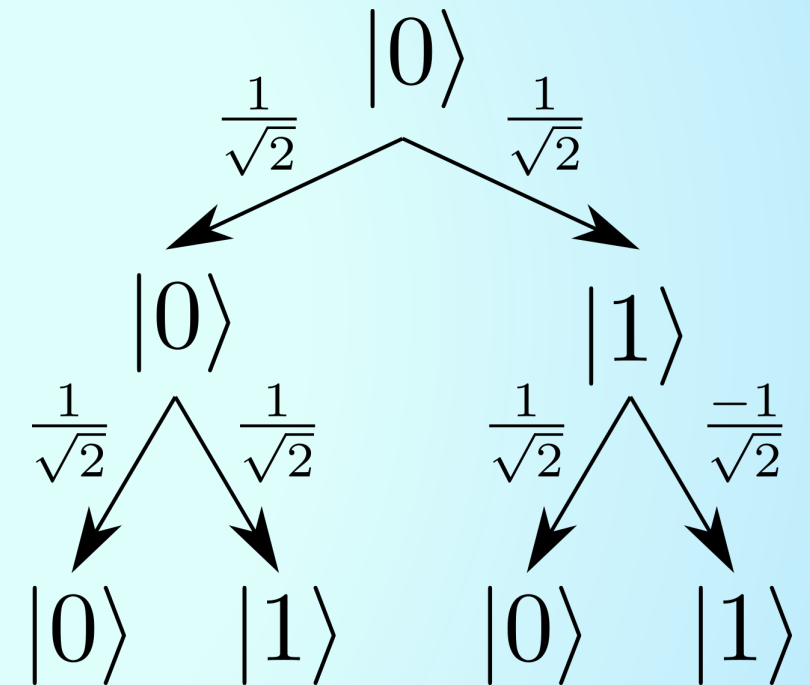
©Johan Jarnestad/The Royal Swedish Academy of Sciences

22/05/2023

Les Interférences - Quantum Interference

Lecture Notes Aaronson

- Many of the most interesting phenomena in quantum mechanics can be explained in terms of quantum interference
- As an illustrative example, suppose we start initially in the $|0\rangle$ state.
- We then apply twice a unitary transformation which when applied to $|0\rangle$ places us in $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and which when applied to $|1\rangle$ places us in $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
- To get the amplitude associated with a particular path we take the product of the amplitudes along that path.
- Then to get the final amplitude associated with a particular output, we sum the amplitudes for each of the paths through the tree leading to that output.
- In this case, the amplitude of $|0\rangle$ is 1 and the amplitude of $|1\rangle$ is 0.
- **The paths leading to $|0\rangle$ interfere constructively while**
- **the paths leading to $|1\rangle$ interfere destructively**



Interférence: le fondement pour la récupération des résultats

22/05/2023

Comment créer des Systèmes Quantiques

Introduction du Qubit Logique

- Pour créer des systèmes quantiques à partir de ces qubits, on manipule les propriétés quantiques de chaque qubit et 'intriquent' (entangle) plusieurs qubits entre eux.
- Ces manipulations sont réalisées à l'aide de **lasers**, de **micro-ondes**, de **champs électriques ou magnétiques** et d'autres moyens de contrôler les qubits.
- Cependant, l'information quantique est **fragile** et peut être irréversiblement perdue par les interactions avec l'environnement, dans un processus appelé **décohérence**.
- Le **temps de cohérence** quantique est la durée pendant laquelle un qubit maintient une superposition ou un état intriqué avant la décohérence, un facteur qui limite la durée pendant laquelle un qubit peut être exploité par une opération.

Qubit Logique

- L'information quantique ne peut pas être copiée (**Théorème de non clonage**) et la mesure perturbe l'information, ce qui empêche la mise en œuvre des techniques classiques de correction des erreurs.
- Les procédures de correction d'erreurs quantiques utilisent de nombreux qubits physiques cibles d'erreurs, et qui travaillent ensemble ainsi qu'avec du traitement classique, afin de créer un système qui se comporte en tant que qubit unique robuste et stable, connu sous le nom de **qubit logique**.

Tableau illustrant
Les ratios qubit
physique/qubit
logique

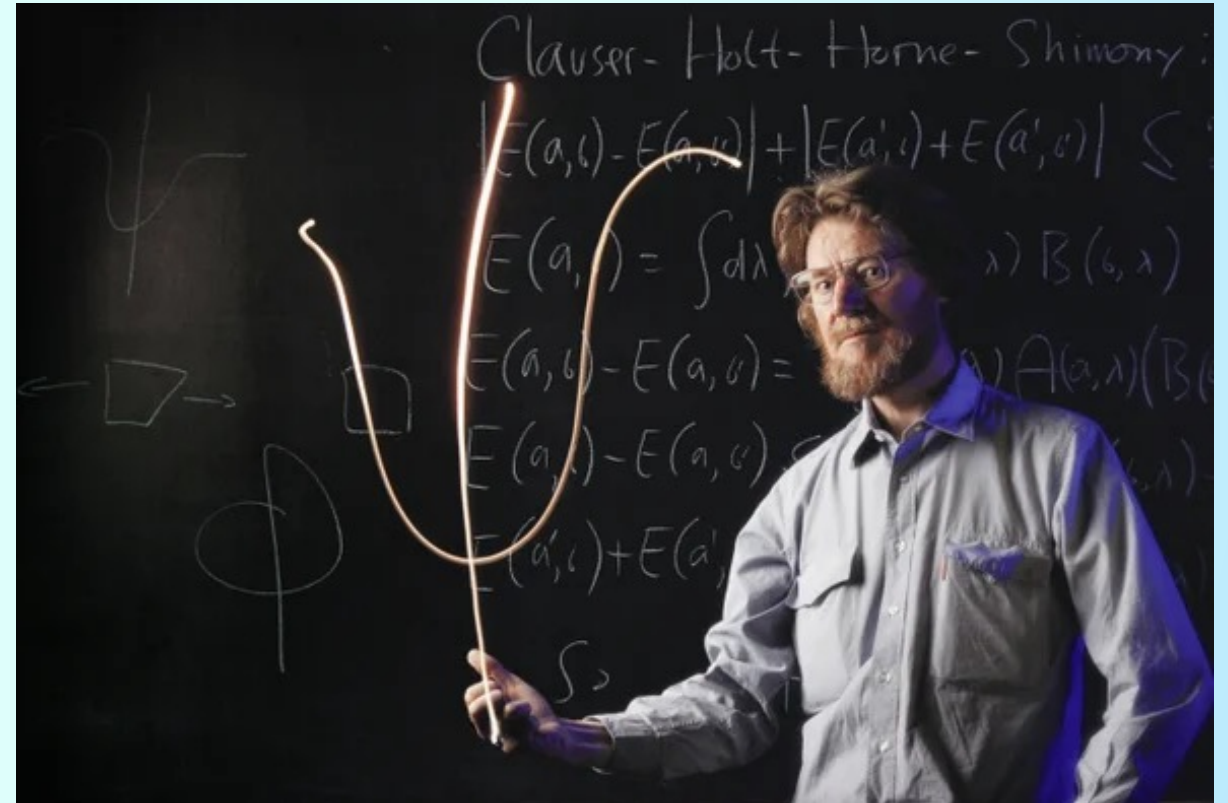
Physical qubit error rate	10^{-3}	10^{-6}	10^{-9}
Physical qubits per logical qubit	15,313	1,103	313
Total physical qubits in processor	1.7×10^6	1.1×10^5	3.5×10^4
Number of T state factories	202	68	38
Number of physical qubits per factory	8.7×10^5	1.7×10^4	5.0×10^3
Total number of physical qubits including T state factories	1.8×10^8	1.3×10^6	2.3×10^5

70 ans après la formalisation de la Mécanique Quantique Les Premiers Cas d'Usage

- ▶ Les inégalités de Bell
- ▶ Teleportation et Codage Superdense
- ▶ Quantum Key Distribution

John Bell

- **Bell's theorem** is the most famous legacy of the late John Bell.
- It is famous for drawing an important line in the sand between quantum mechanics (QM) and the world as we know it intuitively.
- It is simple and elegant and touches upon many of the fundamental philosophical issues that relate to modern physics.
- **No physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics.**

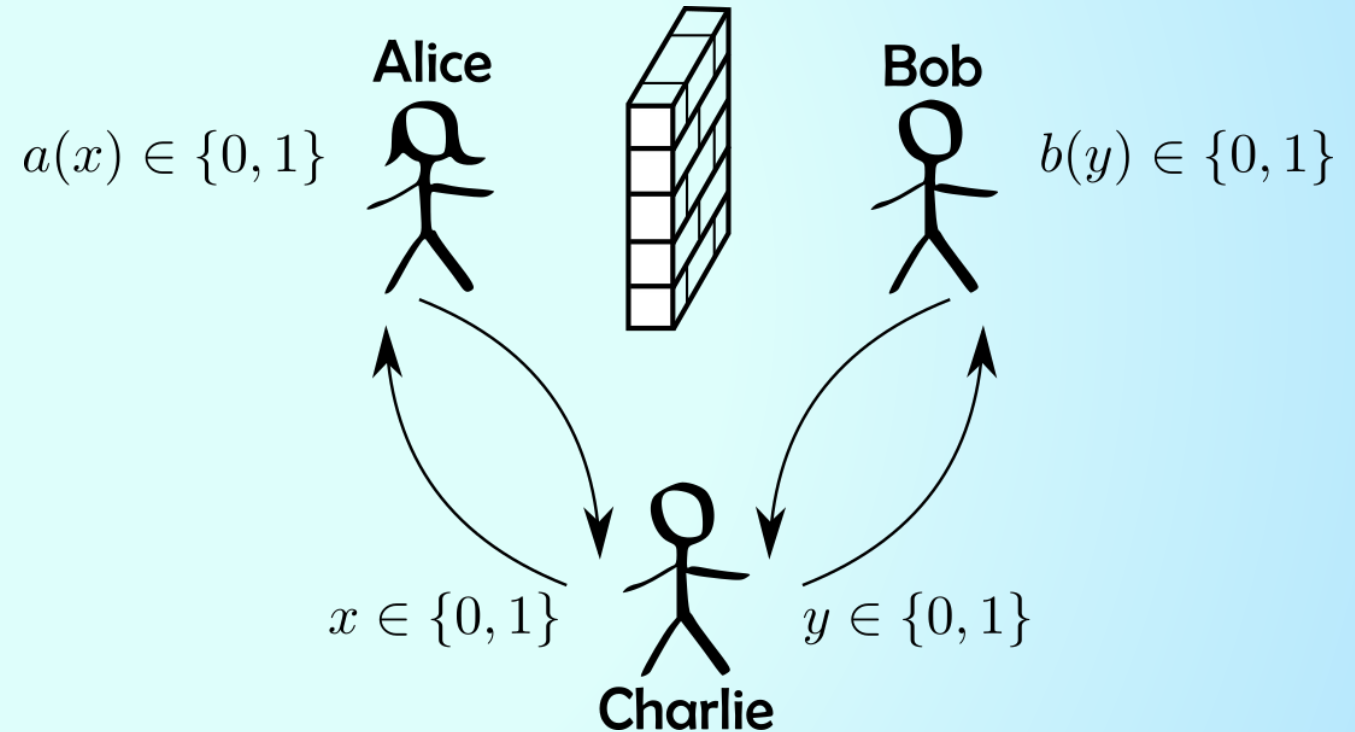


Inégalités de Bell

- Einstein et d'autres avaient déjà émis l'idée de théories de variables cachées locales dans leurs débats philosophiques des années 1930.
- John Bell a été le premier à poser la question suivante : les variables cachées locales ont-elles des conséquences empiriques en désaccord avec les prédictions de la mécanique quantique ?
 - Existe-t-il une expérience réelle qui pourrait exclure la possibilité de variables cachées locales ?
- Bell a proposé une telle expérience, sur un plan conceptuel
- On peut la décrire d'une façon différente de celle de Bell, sur la base d'un jeu/défi avec deux joueurs nommés : Alice et Bob,
- On démontre que la probabilité de résolution est supérieure (grâce à l'intrication partagée) à celle d'une approche classique.
- Ce jeu est appelé le jeu CHSH (Clauser, Horne, Shimony, et Holt)

CHSH Game (Clauser, Horne, Shimony, & Holt)

- Charlie (l'arbitre), prépare deux bits de défi x et y uniformément aléatoires et les envoie respectivement à Alice et Bob.
- En réponse, Alice et Bob renvoient respectivement les bits a et b (qui peuvent dépendre de leurs entrées) à Charlie dans le but d'obtenir $a + b = xy \pmod{2}$.
- Alice et Bob veulent sélectionner des bits de telle sorte que la parité de leurs bits sélectionnés soit égale à l'ET de leurs bits d'entrée.



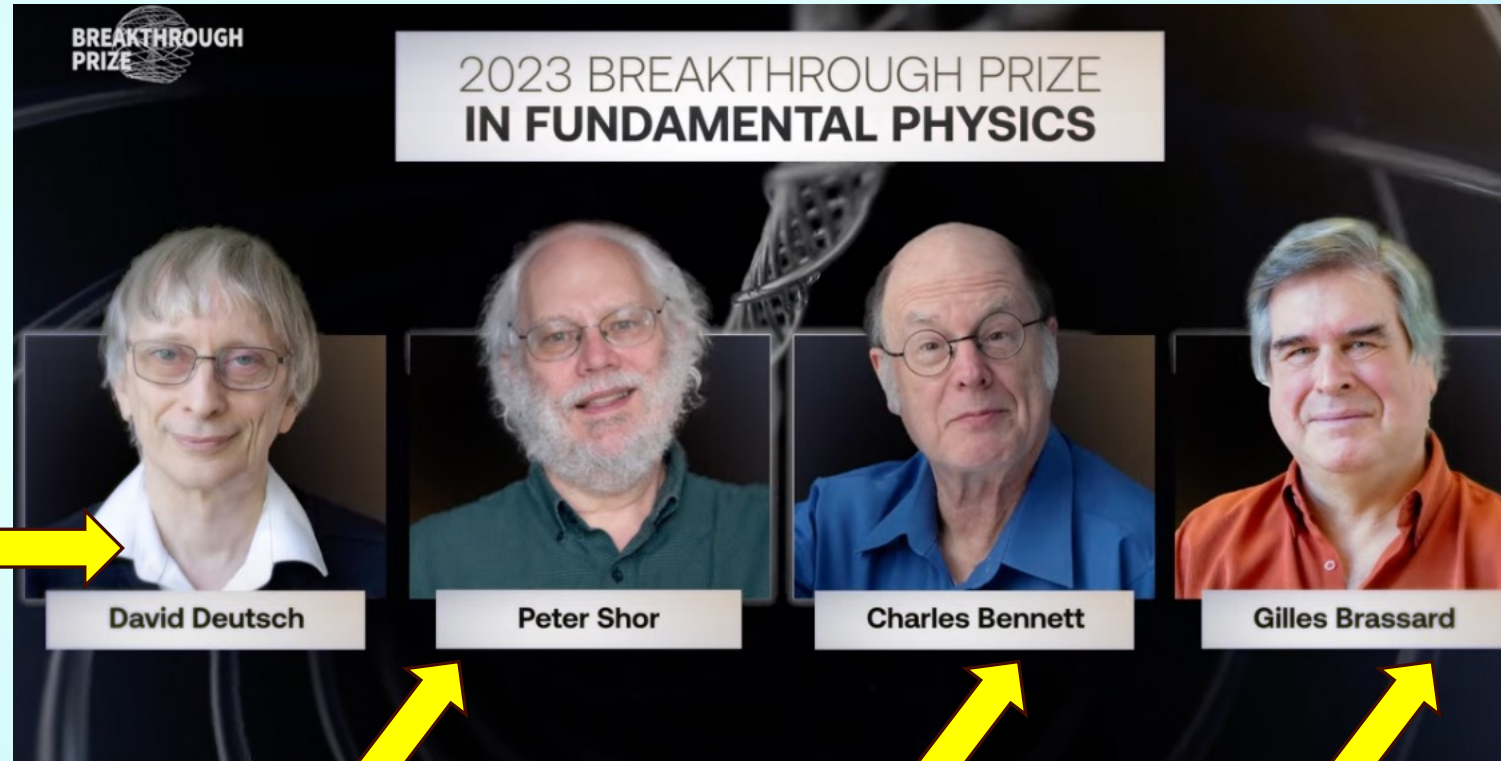
Inégalités de Bell - CHSH Suite

- Une stratégie classique visant à maximiser la probabilité de gagner consiste simplement à ce qu'Alice et Bob envoient toujours à l'arbitre $a = b = 0$, quels que soient x et y . Dans ce cas, Alice et Bob gagnent 75 % du temps, et ne perdent que si x et y sont tous deux égaux à 1.
- L'inégalité de Bell, dans ce cadre, n'est que l'affirmation que la probabilité de victoire classique maximale dans le jeu CHSH est de 75 % et que Si Alice et Bob ont accès à une paire de qubits (EPR) intriqués, il existe une meilleure stratégie. Dans ce cas, en effet, leur probabilité de gain maximale est de

$$P = \cos^2\left(\frac{\pi}{8}\right) \approx 85\%$$

Ceux qui ont mis en évidence la Faisabilité du Quantum Computing, et de ses avantages par rapport l'Informatique Classique (dans certains cas)

QTM
First Algo



David Deutsch

Peter Shor

Charles Bennett

Gilles Brassard

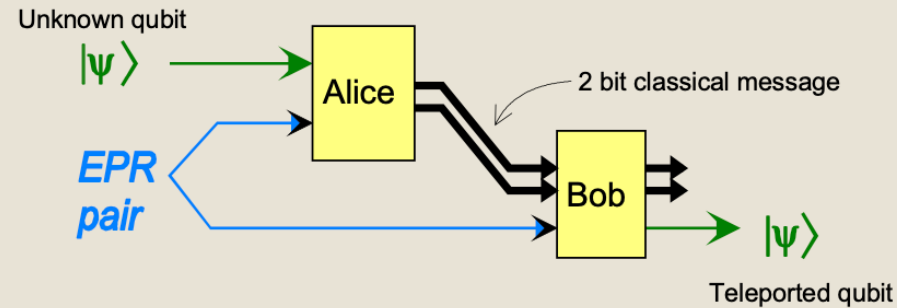
Factorisation
Correction d'erreurs

BB84
QKD
Cryptographie Quantique

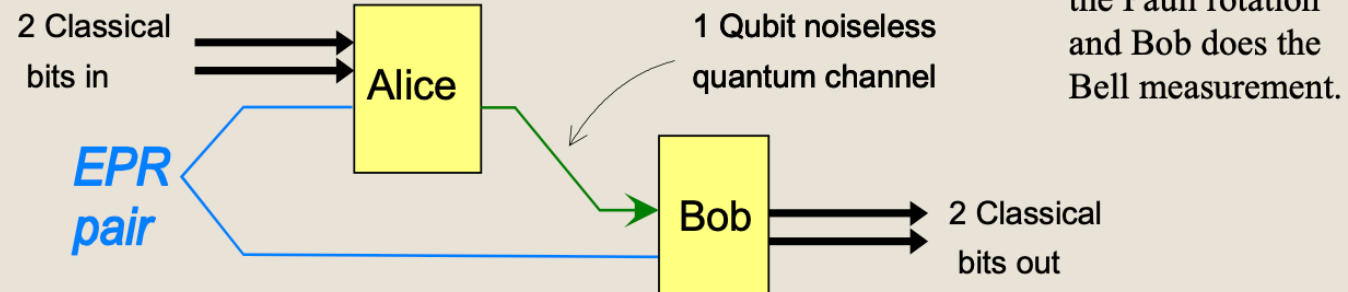
Teleportation & Superdense Coding

A dual process
to teleportation

Quantum Teleportation



Quantum Superdense Coding



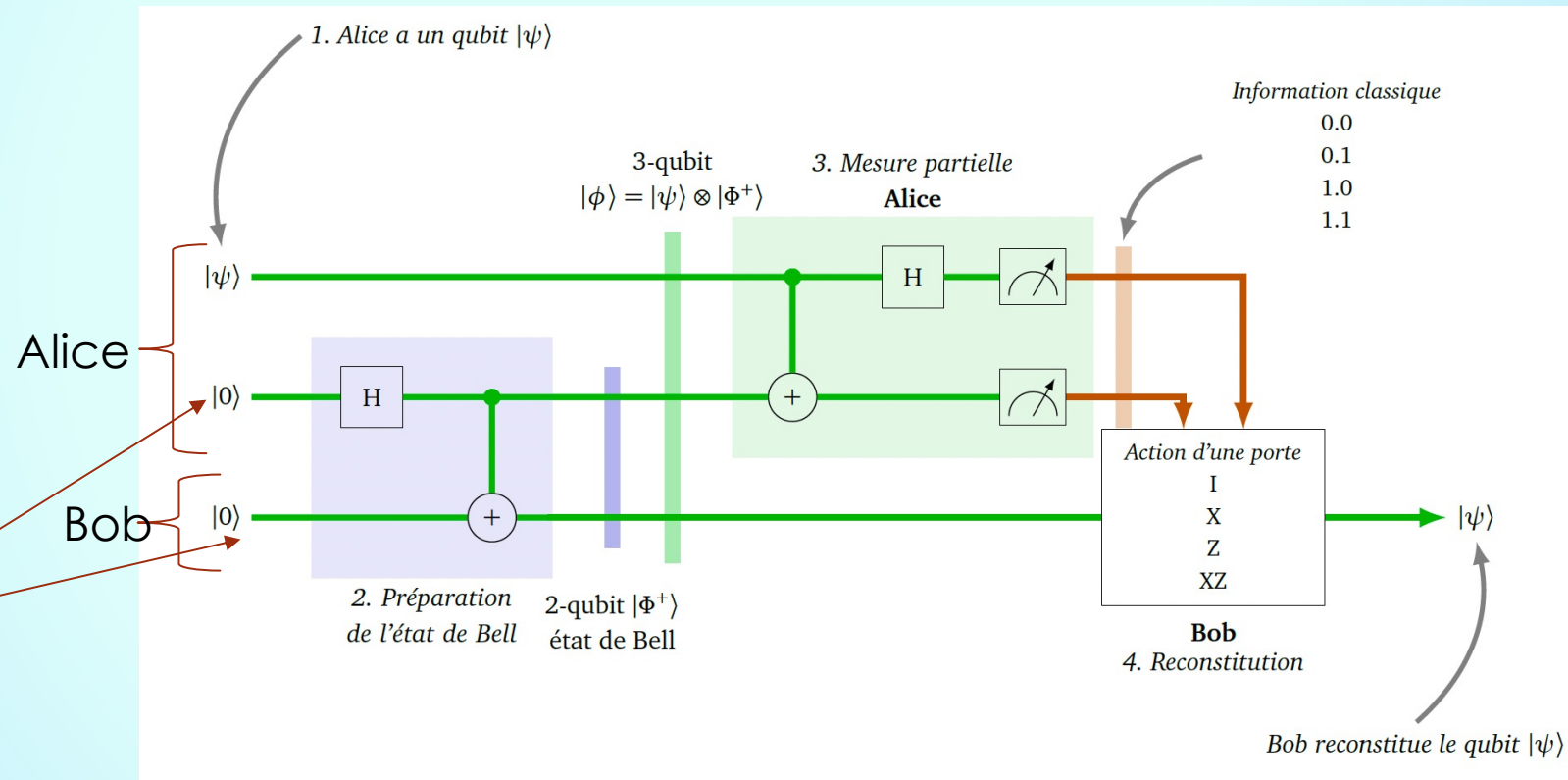
Here Alice does
the Pauli rotation
and Bob does the
Bell measurement.

doubles the classical capacity of any noiseless quantum channel

Téléportation – les Différentes Etapes

Initialisation, Transformations, Mesures

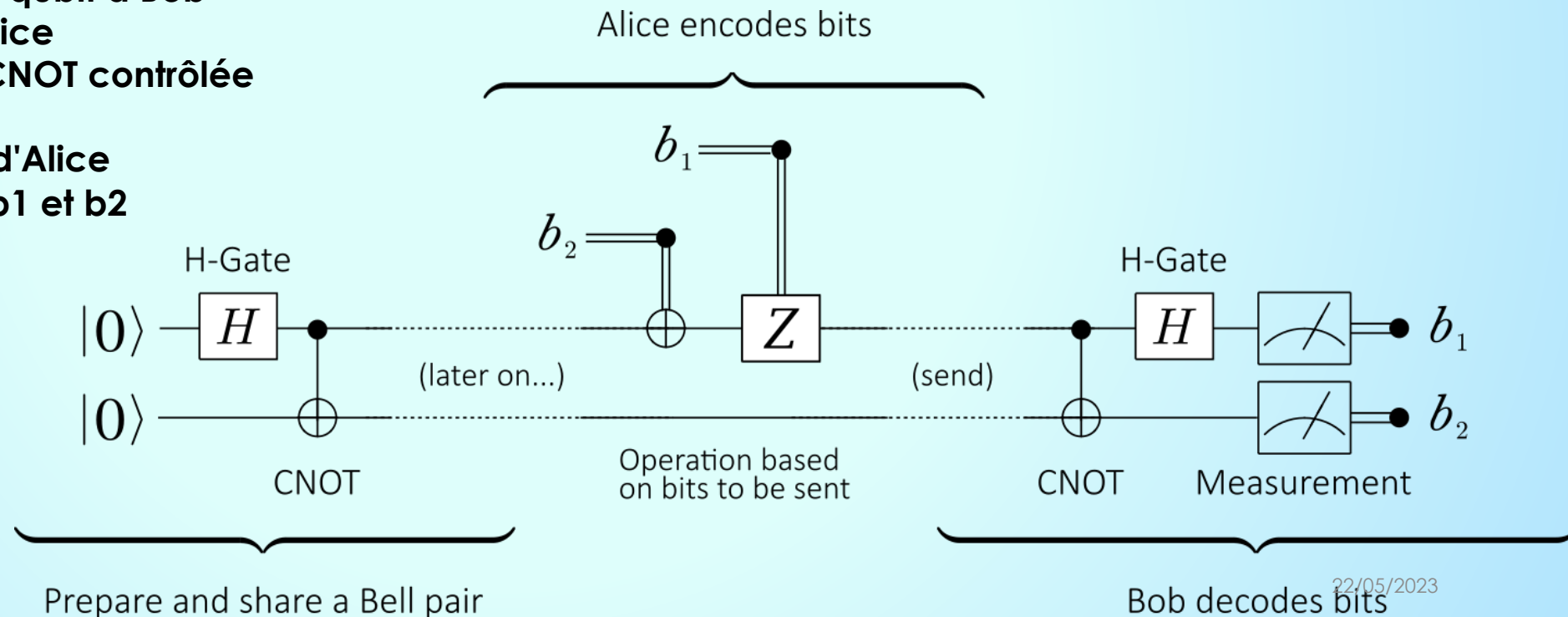
Paire
De qubits
Intriqués
Par H, et +



La téléportation quantique est basée sur une mesure partielle par Alice, qui est en fait une mesure partielle dans la base Bell.

Codage Superdense

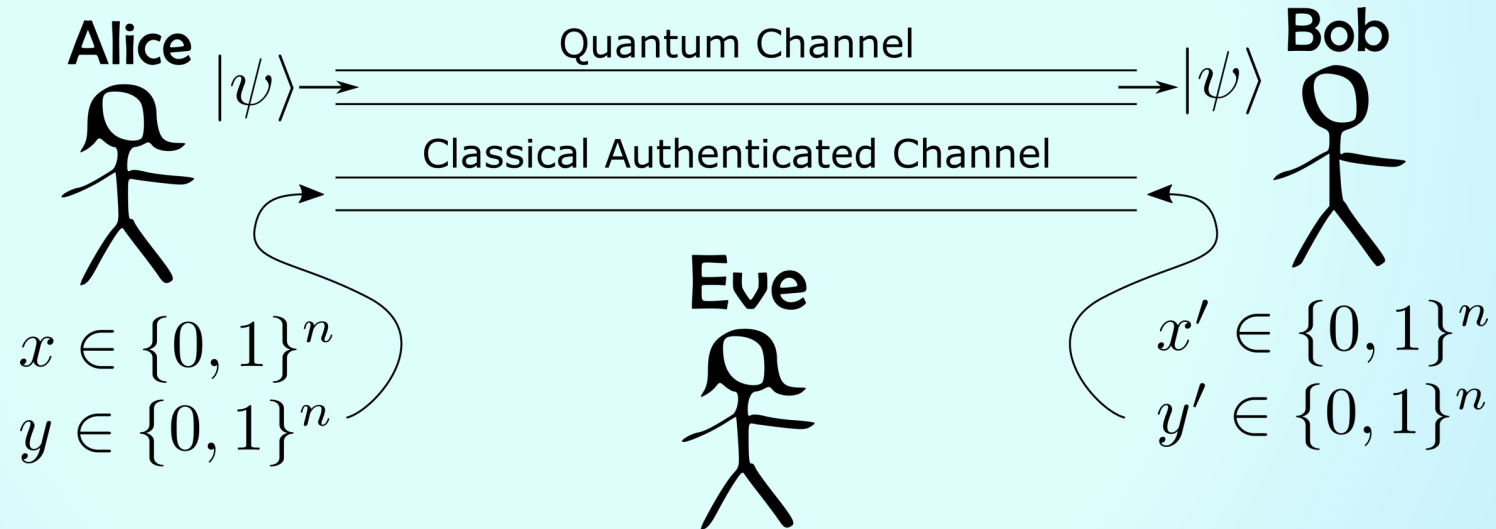
Alice et Bob partagent une paire de Bell à l'avance $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
 Alice veut envoyer à Bob deux bits classiques b_1 et b_2
 Si $b_2 = 1$, elle applique X à son qubit
 Si $b_1 = 1$, elle applique Z à son qubit
 Elle envoie ensuite son qubit à Bob
 Bob reçoit le qubit d'Alice
 Il applique une porte CNOT contrôlée par le qubit d'Alice
 Il applique H au qubit d'Alice
 Il mesure et récupère b_1 et b_2



QKD – Quantum Key Distribution

BB84

En 1984, Charles Bennett et Gilles Brassard ont proposé le premier protocole de distribution de clés quantiques (QKD).



QKD

Basic Quantum Mechanics:

Une mesure quantique perturbe le système

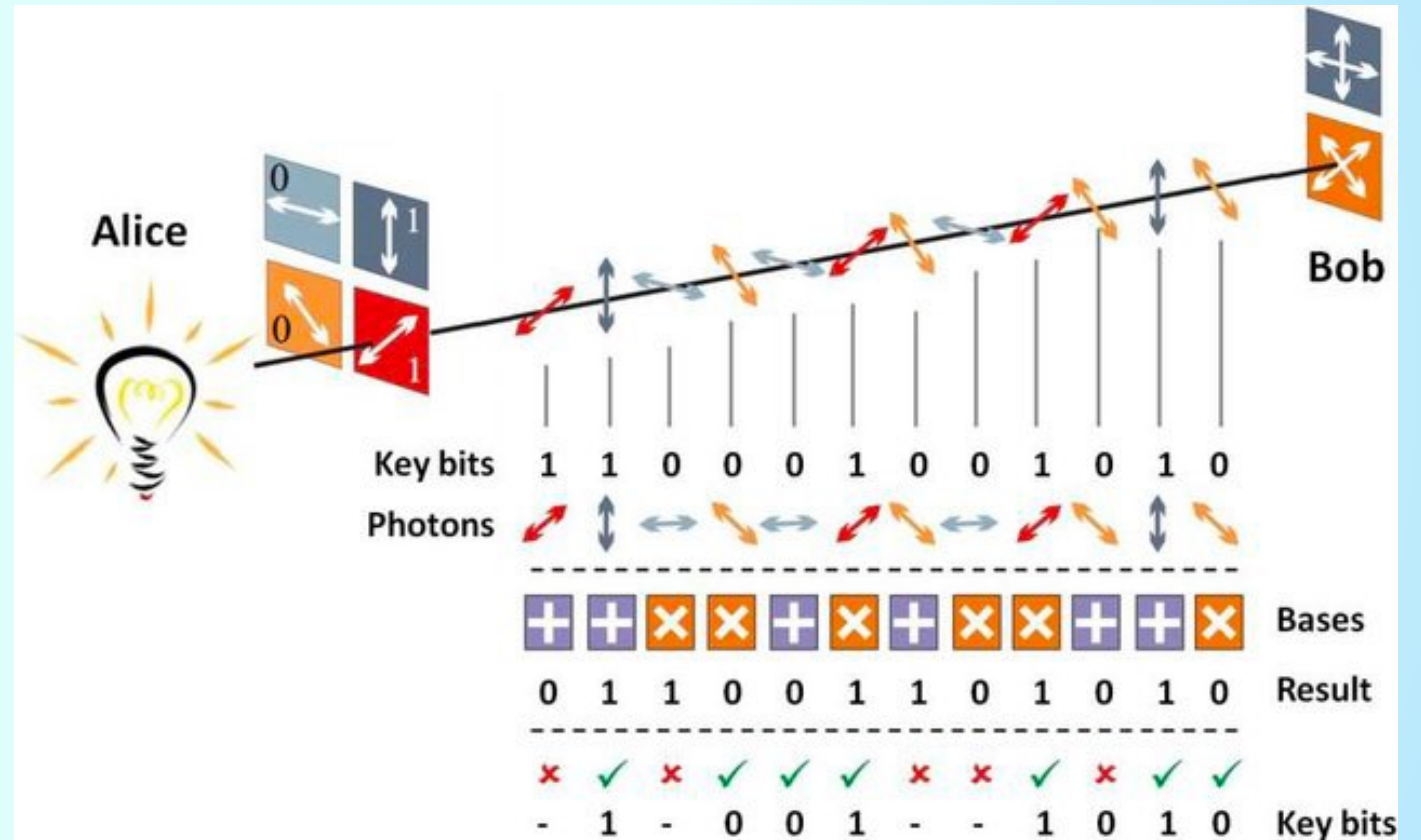
- ▶ Le "canal de communication quantique" n'est pas utilisé pour transmettre un message (information), seule une "clé" est transmise (pas d'information).
- ▶ S'il s'avère que la clé est corrompue, ils ignorent simplement cette clé (aucune information n'est perdue).
- ▶ Si la clé passe avec succès le contrôle, Alice et Bob peuvent l'utiliser en toute sécurité.
- ▶ La confidentialité de la clé est vérifiée avant l'envoi du message.
- ▶ La sécurité de la cryptographie quantique repose sur les fondements de la physique quantique.

QKD suite

- ▶ Si Eve tente d'écouter un "canal de communication quantique", elle doit effectuer des mesures sur des quanta individuels (impulsions de photons uniques).
- ▶ Or, la mécanique quantique nous dit que chaque mesure perturbe le système quantique.
- ▶ Par conséquent, la "lecture" du "signal quantique" par un tiers réduit la corrélation entre les données d'Alice et de Bob.
- ▶ Alice et Bob peuvent donc détecter tout tiers indésirable en comparant (sur un canal public) une partie de leur "signal quantique".

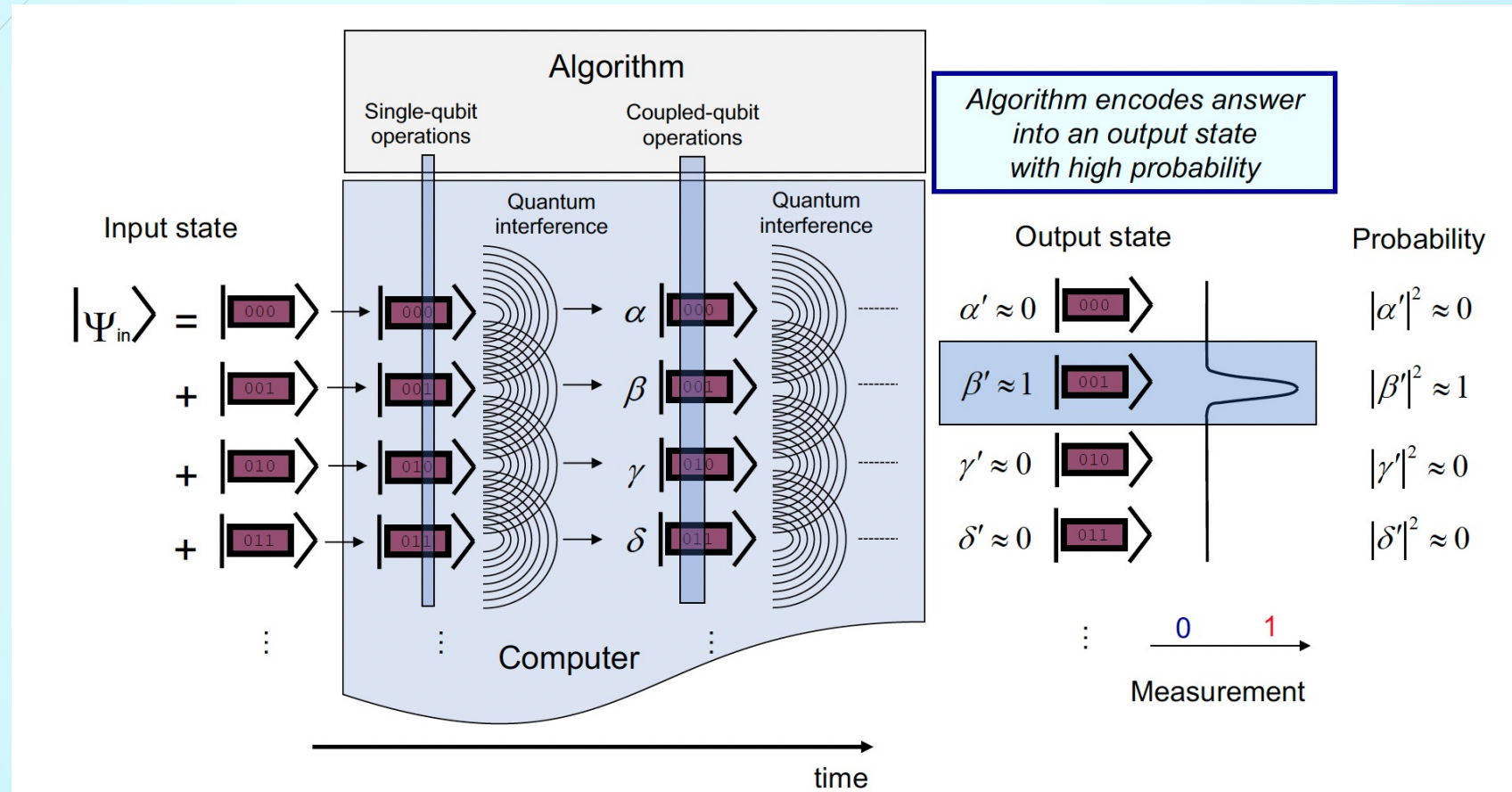
BB84

- Après ce processus, Alice et Bob discutent sur un canal classique (authenticé mais pas nécessairement sécurisé)
- Bob annonce les bases qu'il a utilisées pour ses mesures et Alice annonce les bases qu'elle a utilisées pour coder les bits .
- Bob n'annonce PAS les résultats de ses mesures
- Pour les bits pour lesquels Bob a mesuré avec la même base que celle qu'Alice a utilisée pour le codage, **il a obtenu le bit qu'Alice avait l'intention d'envoyer**
- Les autres sont rejetés
- Ils garderont environ la moitié des bits



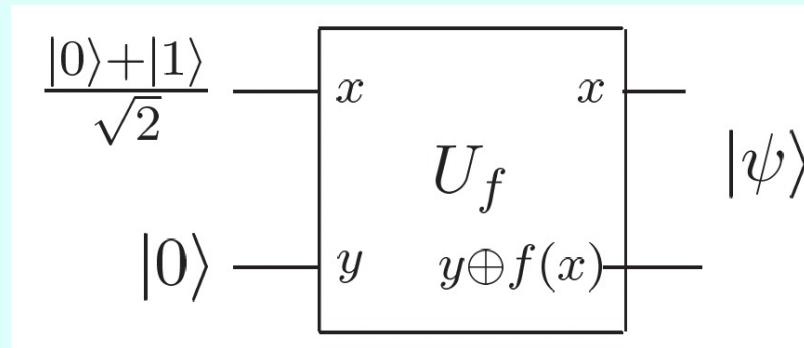
Les Algorithmes

Quantum Algorithm (universal)



Le Parallélisme quantique

Le parallélisme quantique est une caractéristique fondamentale de nombreux algorithmes. D'un point de vue heuristique, le parallélisme quantique permet aux ordinateurs quantiques d'évaluer une fonction $f(x)$ pour différentes valeurs de " x " **simultanément**.



Supposons $f(x) : \{0, 1\} \rightarrow \{0, 1\}$ est une fonction de 1 bit (portée et domaine)

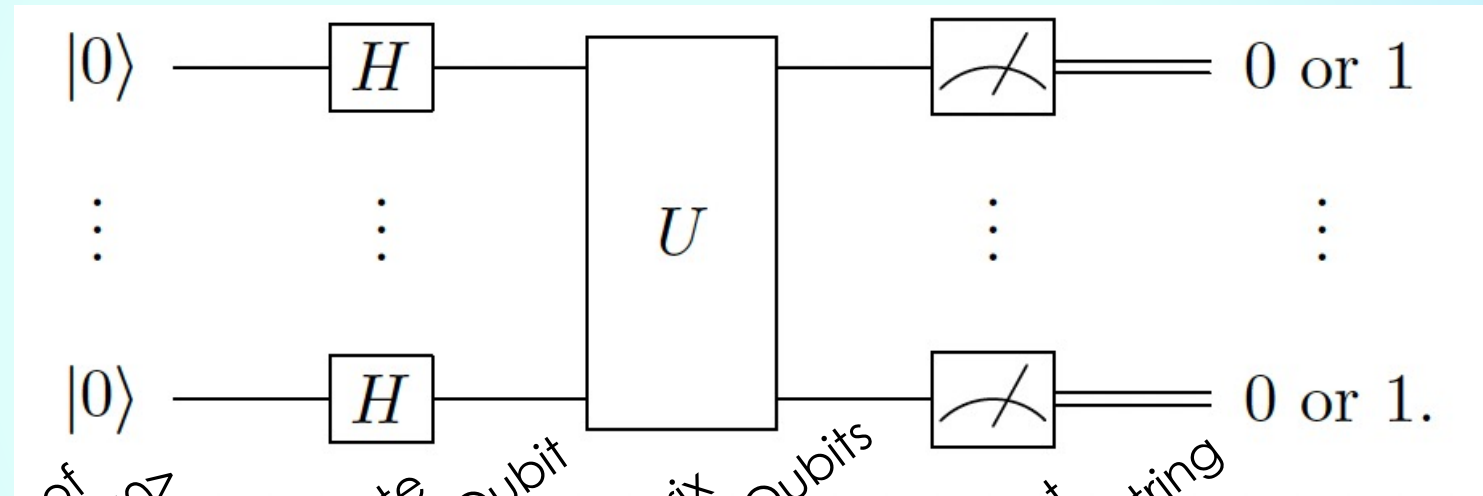
Une façon pratique de calculer cette fonction sur un ordinateur quantique est de considérer un OQ à deux qubits qui commence dans l'état $|x, y\rangle$. Avec une séquence appropriée de portes logiques, il est possible de transformer cet état en $|x, y \oplus f(x)\rangle$, où $\oplus$ indique une addition modulo 2 ; le premier registre est appelé registre de "données", et le second registre le registre de "cible".

Nous donnons à la transformation définie par le renvoi $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ un nom, U_f , et notons qu'il est facile de montrer qu'elle est unitaire.

Si $y = 0$, alors l'état final du second qubit est simplement la valeur $f(x)$.

Standard model of quantum computing

Portugal Basic QC book



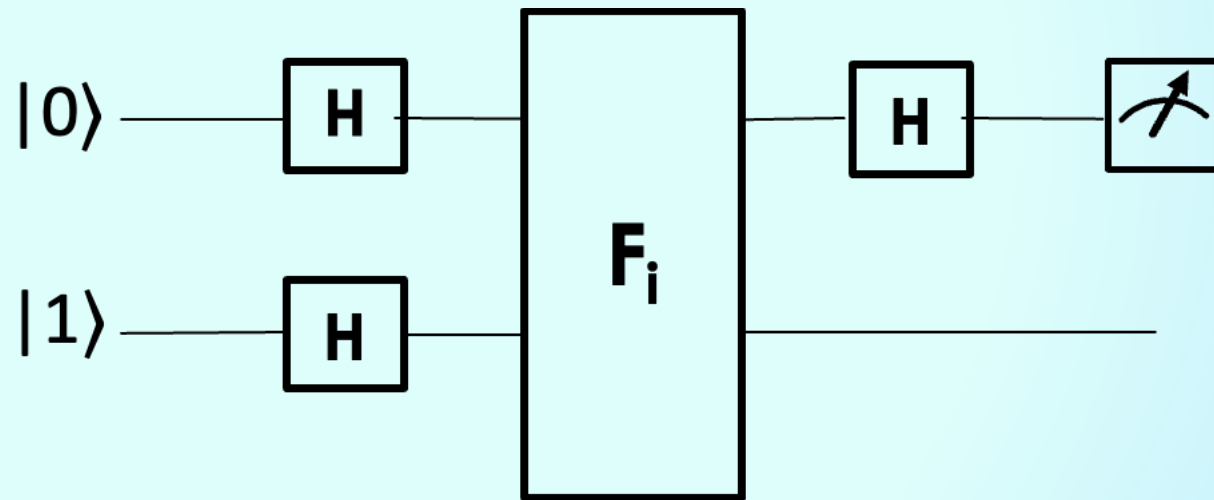
Initial State of
each Qubit is $|0\rangle$

Hadamard Gate
Applied to each Qubit

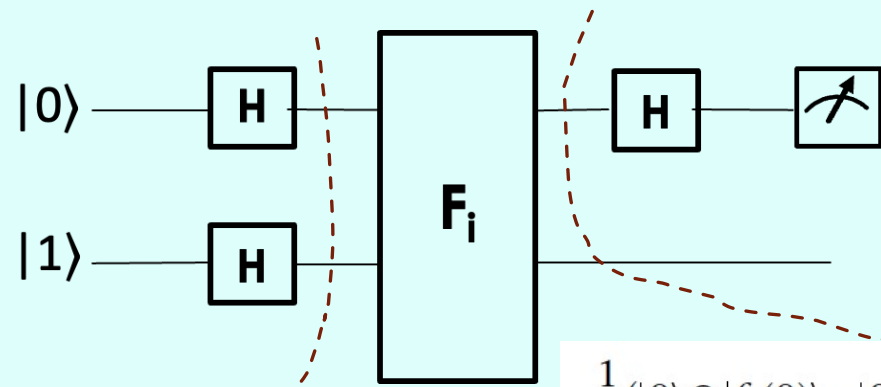
Unitary Matrix
Applied to all Qubits

Measurement
Returning a bit string

La Beauté des Portes (Gates) et des Circuits



La Beauté de l'Habillage Mathématique 😊



$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

$$\frac{1}{2}(|0\rangle \otimes |f_i(0)\rangle - |0\rangle \otimes |f_i(0) \oplus 1\rangle + |1\rangle \otimes |f_i(1)\rangle - |1\rangle \otimes |f_i(1) \oplus 1\rangle).$$

$$\frac{1}{2}(|0\rangle \otimes (|f_i(0)\rangle - |f_i(0) \oplus 1\rangle) + |1\rangle \otimes (|f_i(1)\rangle - |f_i(1) \oplus 1\rangle))$$

$$|f_i(0)\rangle - |f_i(0) \oplus 1\rangle = (-1)^{f_i(0)} (|0\rangle - |1\rangle)$$

$$|f_i(1)\rangle - |f_i(1) \oplus 1\rangle = (-1)^{f_i(1)} (|0\rangle - |1\rangle).$$

$$\frac{1}{2}(|0\rangle \otimes ((-1)^{f_i(0)} (|0\rangle - |1\rangle)) + |1\rangle \otimes ((-1)^{f_i(1)} (|0\rangle - |1\rangle))).$$

22/05/2023

Les Algorithmes

- 1985 **David Deutsch** paper P Turing Machine
- 1992 **David-Jozsa** deterministic quantum advantage
- 1993 **Vazirani et Bernstein** nondeterministic quantum advantage & Quantum Fourier Transform description
- 1994 **Daniel Simon** - Period Finding problem
- 1994 **Peter Shor** - Bell Labs factoring large number
- 1996 **Lov Grover** search algorithm quadratic speedup on QC (OVN)
- 1996 **Farhi & Gutman** Hamiltonian version of Grover algorithm

Les Algorithmes Quantiques - Le Début

1985
Deutsch

1992
Deutsch –
Jozsa

1993
Bernstein
Vazirani

1994 Simon

1994 Shor

1995 Kitaev

1996 Grover

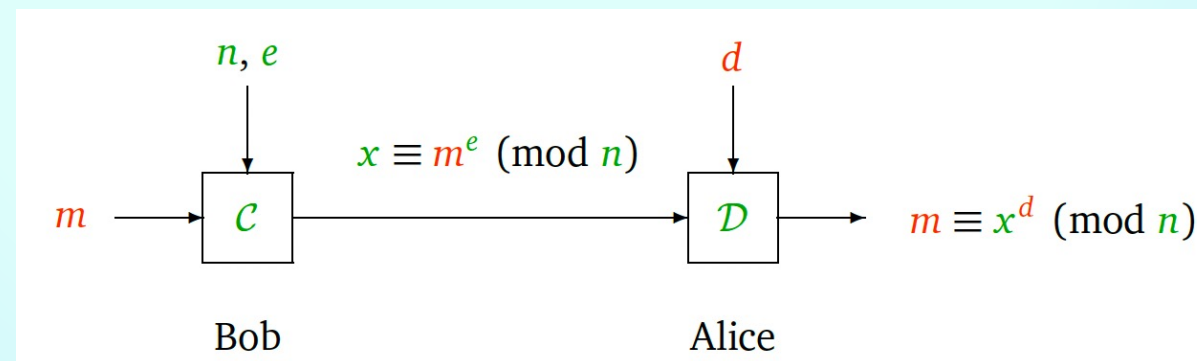
Seront traités dans un futur
séminaire



Shor

RSA chiffrement et le déchiffrement

- n , e forment la clé publique d'Alice
- d est la clé privée d'Alice,
- m est le message secret que Bob souhaite transmettre à Alice,
- x est le message chiffré que Bob calcule à partir de la clé publique d'Alice et qu'il lui transmet,
- seule Alice peut retrouver m par un calcul à partir de x et de sa clé privée d .



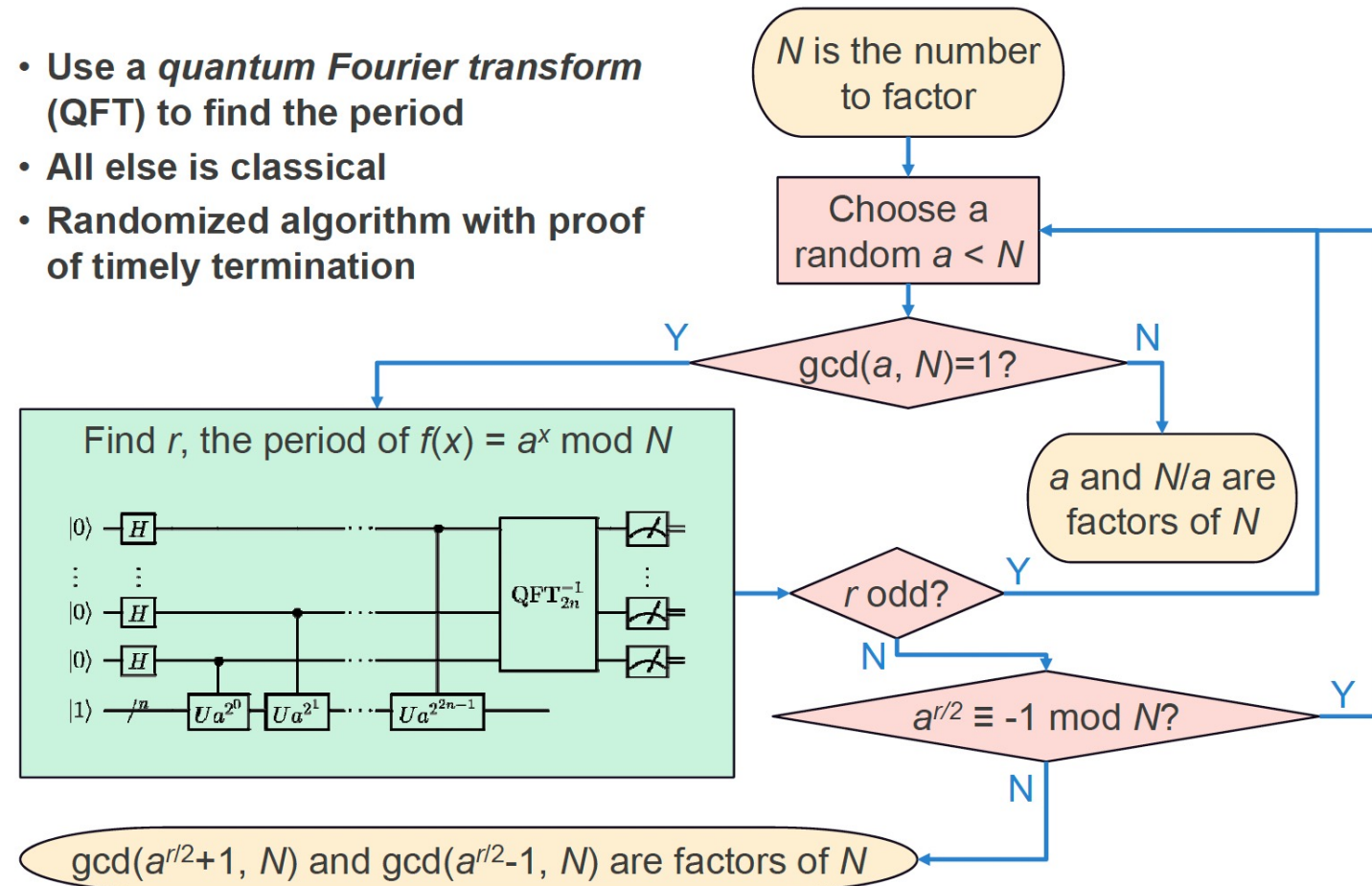
Choix de deux nombres premiers

- ▶ Alice effectue, une fois pour toutes, les opérations suivantes (en secret) :
- ▶ elle choisit deux nombres premiers distincts p et q (dans la pratique ce sont de très grands nombres, jusqu'à des centaines de chiffres),
- ▶ elle calcule $n = p * q$,
- ▶ elle calcule $\varphi(n) = (p - 1) * (q - 1)$.
- ▶ Vous noterez que le calcul de $\varphi(n)$ n'est possible que si la décomposition de n sous la forme $p * q$ est connue.
- ▶ D'où le caractère secret de $\varphi(n)$ même si n est connu de tous

Shor – Algorithme Hybride combinant IT Classique et IT Quantique

Shor's Algorithm (cont.)

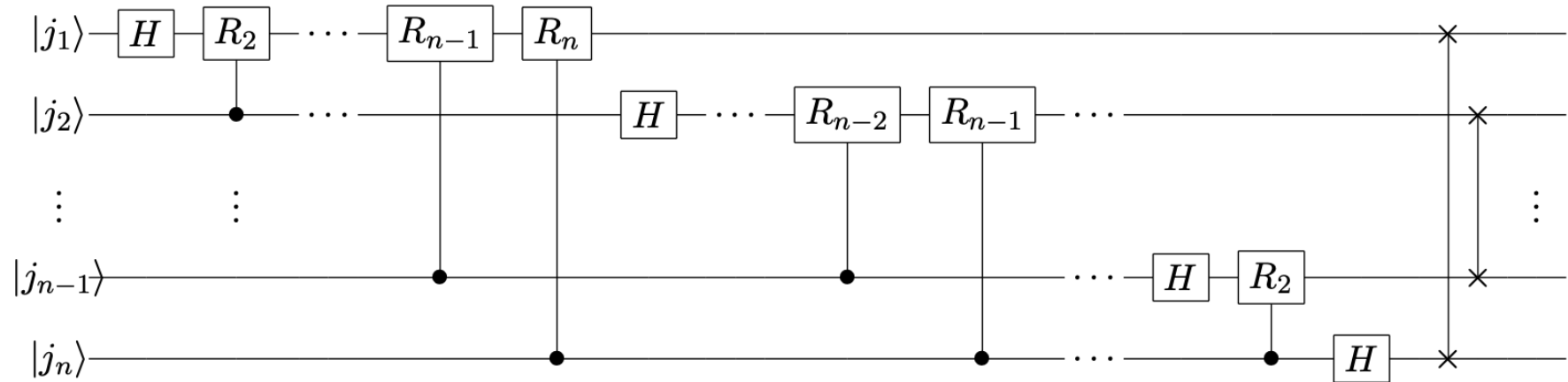
- Use a *quantum Fourier transform* (QFT) to find the period
- All else is classical
- Randomized algorithm with proof of timely termination



QFT – Le Circuit Quantique

The QFT of order m is the unitary transformation defined by
 The number of gates is quadratic in m , an exponential
 speed-up over the classical case (FFT)
 For Shor, m can be chosen to be about $2n$

$$QFT |j\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} e^{\frac{2\pi i j k}{2^m}} |k\rangle$$



Pour casser RSA et le ECDSA (Discrete Log)

TABLE 4.1 Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required ^a	Time Required to Break System ^b	Quantum-Resilient Replacement Strategies
AES-GCM ^c	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} years 1.97×10^{22} years 2.29×10^{32} years	
RSA ^d	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,050 4,098 8,194	8.05×10^6 8.56×10^6 1.12×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete-log problem ^{e-g}	Asymmetric encryption	256 384 521	128 192 256	Shor's algorithm	2,330 3,484 4,719	8.56×10^6 9.05×10^6 1.13×10^6	10.5 hours 37.67 hours 55 hours	Move to NIST-selected PQC algorithm when available
SHA256 ^h	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iterations ⁱ	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

RSA - Internet

ECDSA Bitcoin

La Suite des Algorithmes

VQE

Simulation
Chemistry

QAOA

Seront traités dans un futur
séminaire

QPE

ML

HHL

QRNG

Quantum
Walks

Résumé des Algorithmes Avancés

en cours de développement, et exploitant les résultats des Algorithmes Fondamentaux de la 1ère Génération (D, DJ, BV, Grover, Simon,

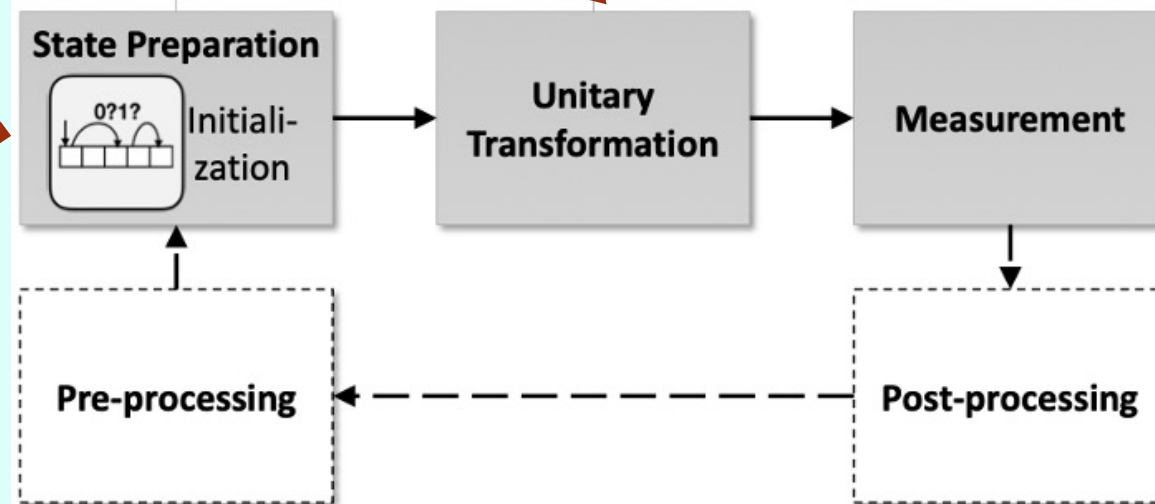
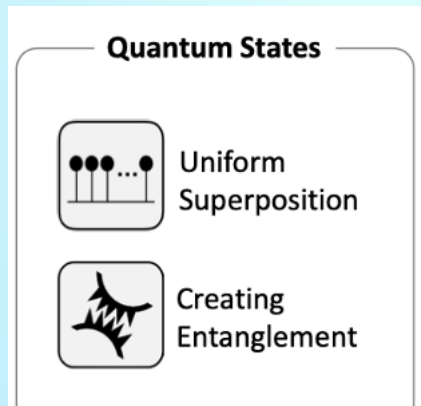
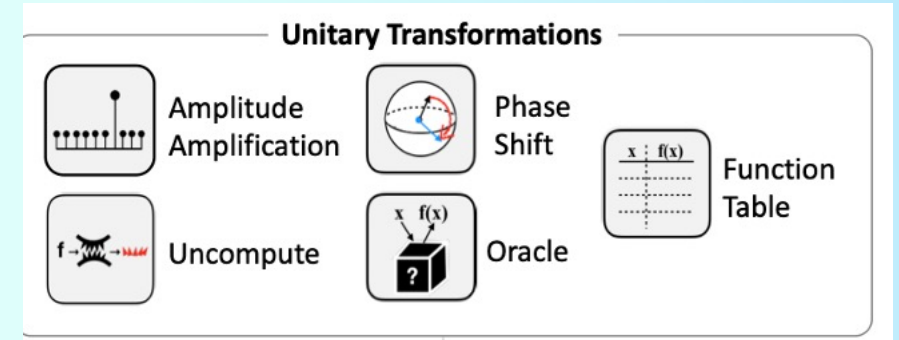
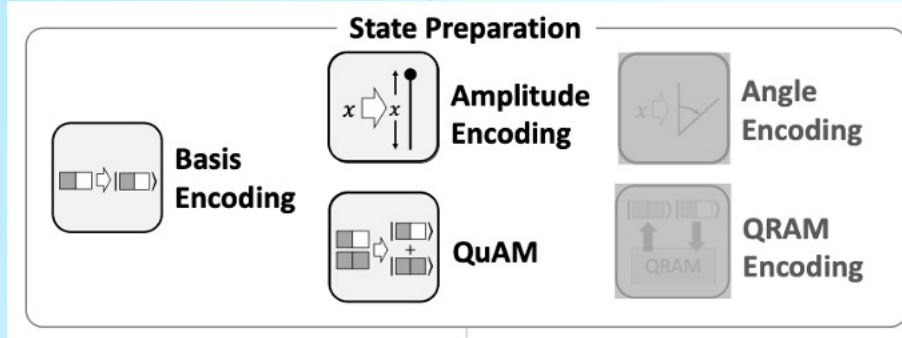
Class	Problem/Algorithm	Paradigms used	Hardware	Simulation Match
Inverse Function Computation	Grover's Algorithm	GO	QX4	med
	Bernstein-Vazirani	n.a.	QX4, QX5	high
Number-theoretic Applications	Shor's Factoring Algorithm	QFT	QX4	n.a.
Algebraic Applications	Linear Systems	HHL	QX4	n.a.
	Matrix Element Group Representations	QFT	QX4	n.a.
	Matrix Product Verification	GO	QX4	n.a.
	Subgroup Isomorphism	QFT	QX4	n.a.
	Persistent Homology	GO, QFT	QX4	med-low
Graph Applications	Quantum Random Walk	n.a.	VIGO	med-low
	Minimum Spanning Tree	GO	QX4	med-low
	Maximum Flow	GO	QX4	med-low
	Approximate Quantum Algorithms	SIM	QX4	high
Learning Applications	Quantum Principal Component Analysis (PCA)	QFT	QX4	med
	Quantum Support Vector Machines (SVM)	QFT	none	n.a.
	Partition Function	QFT	QX4	med-low
Quantum Simulation	Schrödinger Equation Simulation	SIM	QX4	low
	Transverse Ising Model Simulation	VQE	none	n.a.
Quantum Utilities	State Preparation	n.a.	QX4	med
	Quantum Tomography	n.a.	QX4	med
	Quantum Error Correction	n.a.	QX4	med

Seront traités dans un futur séminaire

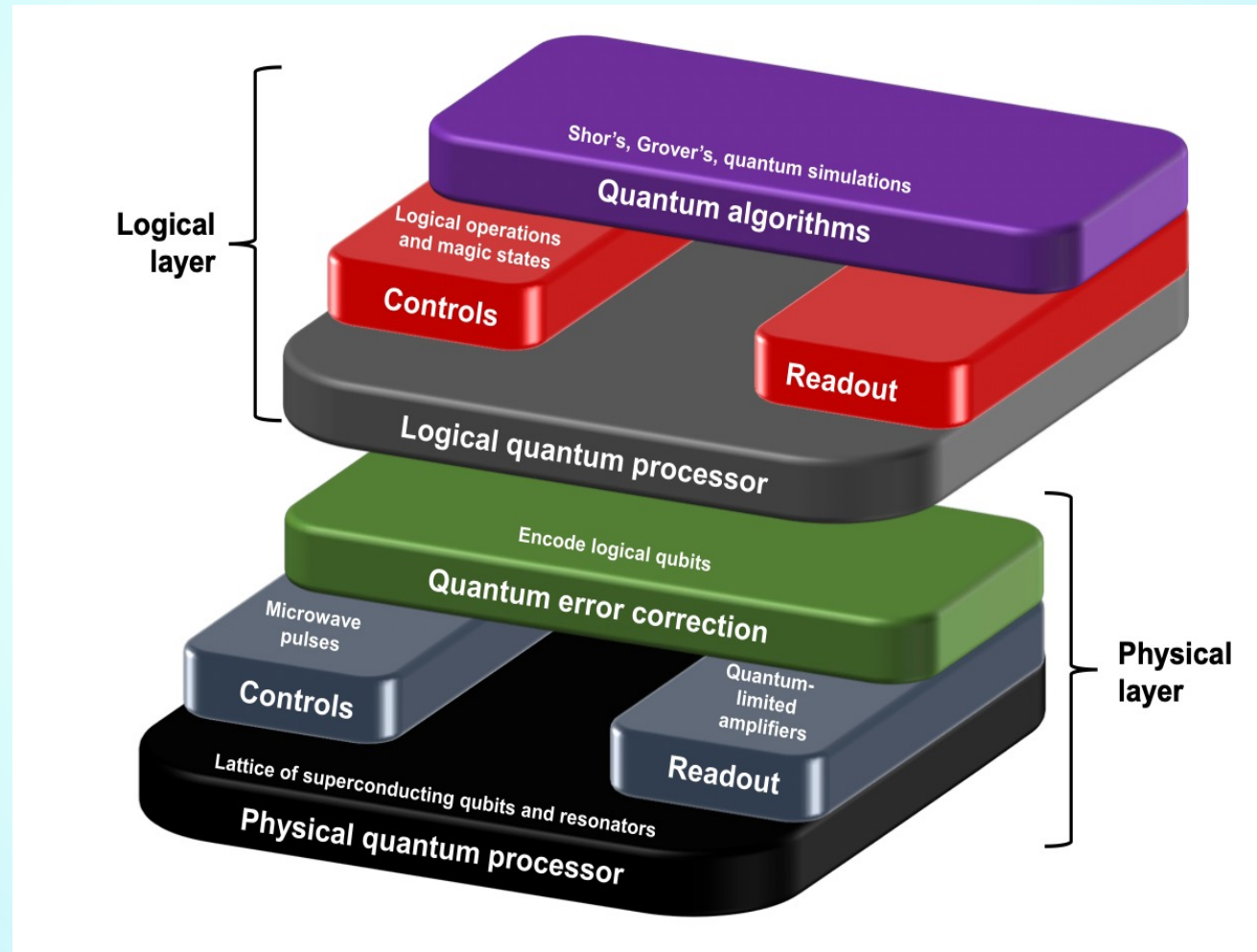
Les Thèmes Applicatifs

Paradigms include Grover Operator (GO), Quantum Fourier Transform (QFT), Harrow-Hassidim-Lloyd (HHL), Variational Quantum Eigenvalue solver (VQE), and direct Hamiltonian simulation (SIM). The simulation match column indicates how well the hardware quantum results matched the simulator results

Les Différents Etapes d'un Algorithme

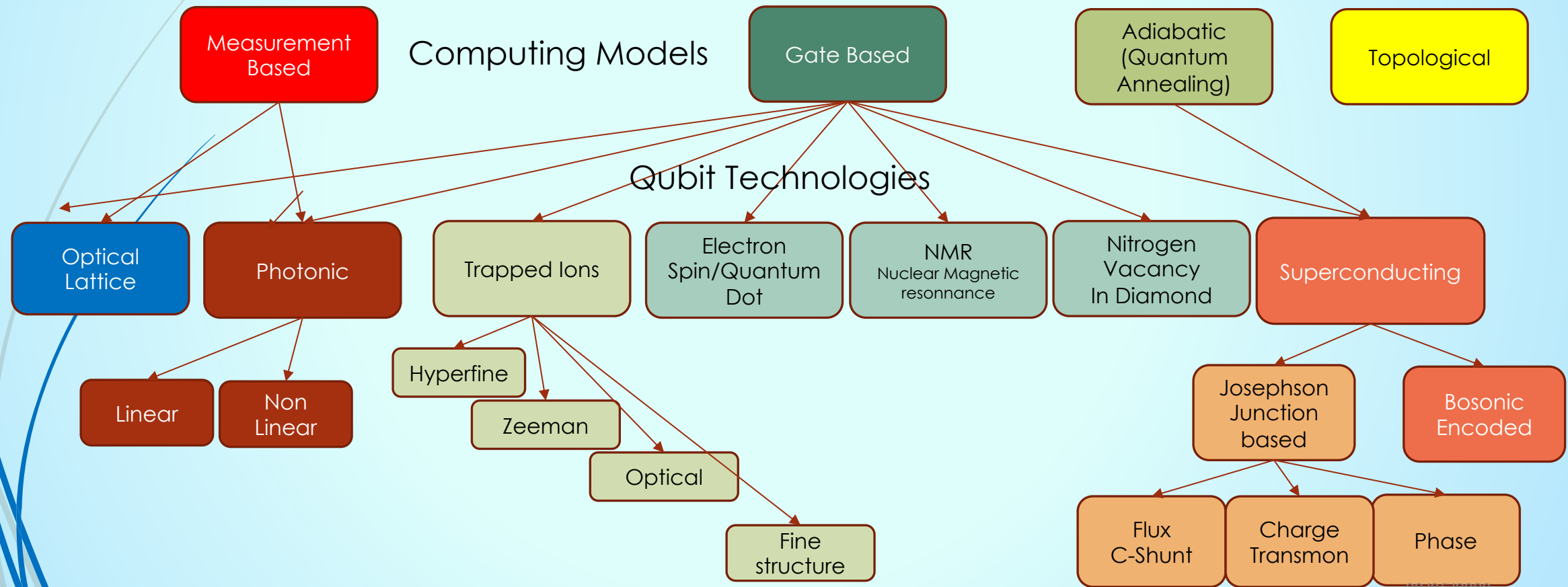


Constitution d'un Système Quantique



Le Hardware

Computing Models and Qubit Technologies



Construire un Ordinateur Quantique

Critères

- Universalité
- Fidélité
- Scalabilité
- Nombre de Qubits
- Profondeur du circuit
- Connectivité logique

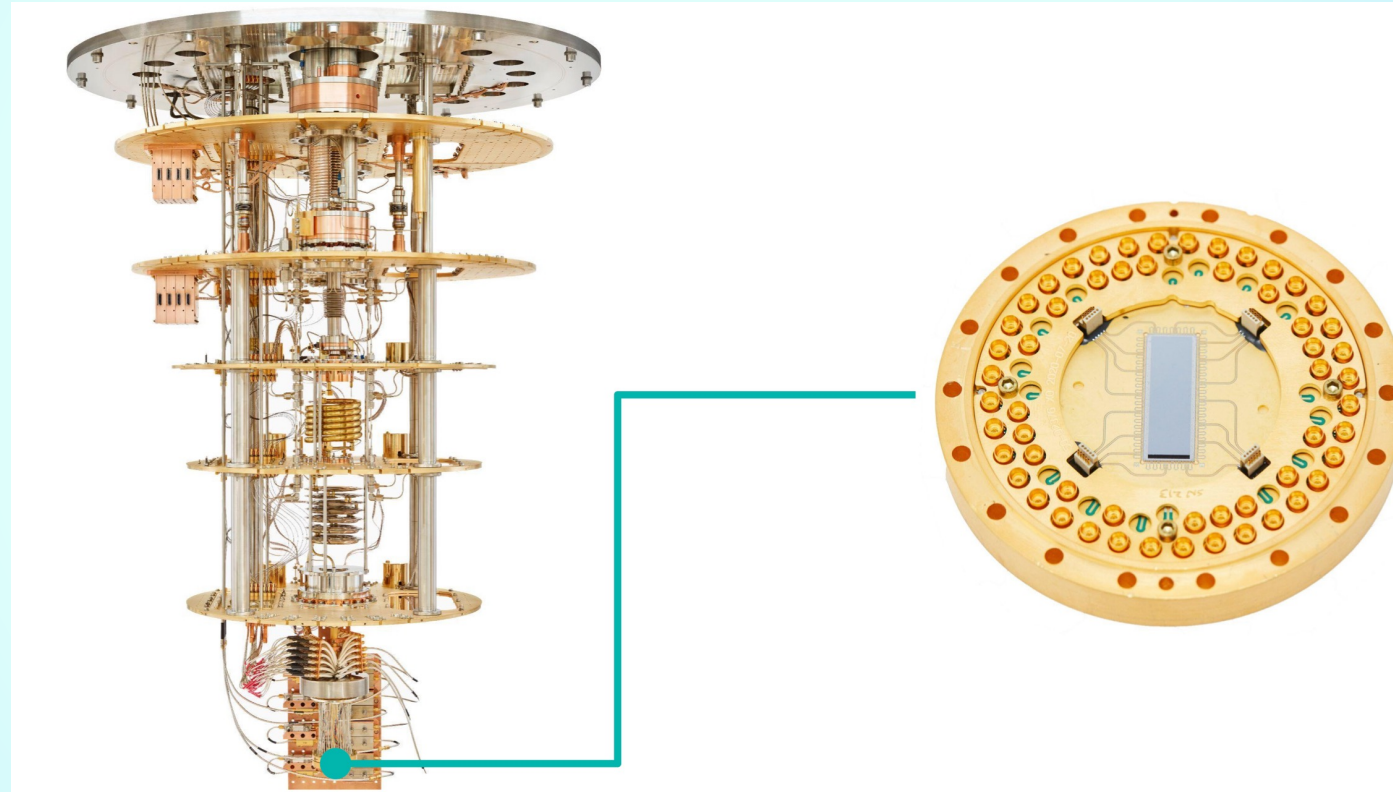
Modèles Physiques

- Ordinateurs quantiques à ions piégés
- Ordinateurs quantiques adiabatiques - «recuit quantique»
- Ordinateurs quantiques optiques
- Ordinateurs quantiques à supraconduction
- Ordinateurs quantiques topologiques

Les Critères à Satisfaire pour construire un Ordinateur Quantique

- Système physique Scalable avec des qubits bien définis,
- Capacité à initialiser les qubits dans un état simple,
- Robustesse au bruit ambiant : temps de décohérence longs, bien plus longs que le temps de fonctionnement de la porte,
- Capacité à réaliser des portes quantiques universelles de haute fidélité,
- Mesures spécifiques aux qubits à haute efficacité.
- Capacité d'interconvertir des qubits stationnaires et volants,
- Transmission fidèle de qubits volants entre des emplacements spécifiés

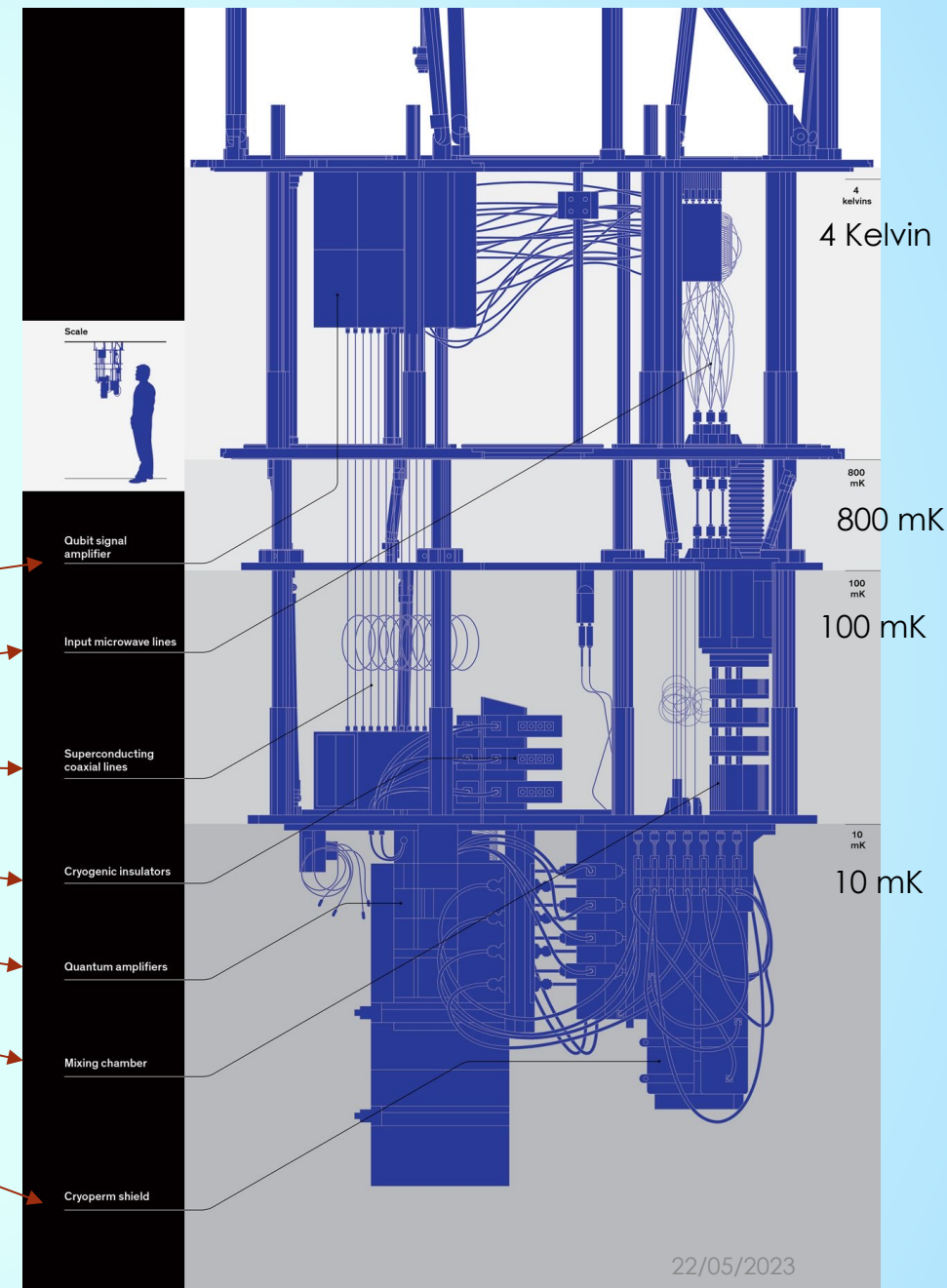
La Puce Quantique au centre !



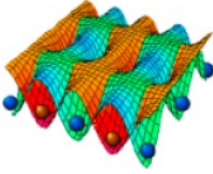
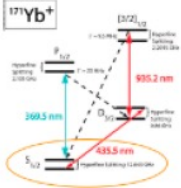
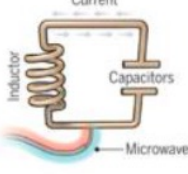
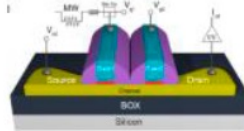
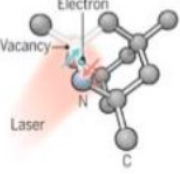
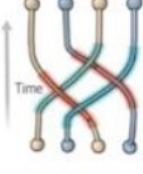
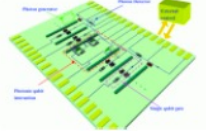
Le Froid

QC must be chilled to near absolute zero temperature to function. That cooling is accomplished using a dilution refrigerator

Qubit signal Amplifier
Input Microwave lines
Superconducting coaxial Lines
Cryogenic Insulators
Quantum Amplifiers
Mixing chamber
Cryoperm shield



A mettre à jour

	atoms		electrons superconducting & spins				photons
							
	cold atoms	trapped ions	superconducting	silicon	NV centers	Majorana fermions	photons
qubit size	about 1 μm space between atoms	about 1 μm space between atoms	$(100\mu)^2$	$(100\text{nm})^2$	$<(100\text{nm})^2$	$(100\mu)^2$	$(100\mu)^2$
two gates fidelities	98%	99,9%	99,4%	$>98\%$	99,2%	N/A	98%
readout fidelity	99%	99,9%	99,4%	98%	98%	N/A	50%
gate time	1 μs	100 μs	20 ns - 300 ns	$\approx 5 \mu\text{s}$	10-700 ns	N/A	1 ms
coherence		0,2s-10mn	100-400 μs	20-120 μs	2.4 ms	N/A	
qubits temperature	$< 5\text{mK}$	$<1\text{mK}$ to 10K	15mK	100mK-1K	4K-ambient	15mK	ambient & 4K/10K photons generators & detectors
operational qubits	100-196 (simulator)	32 (IonQ)	65 (IBM) 56-66 (China)	4 (Delft)	5 (Quantum Brilliance)-10	N/A	70 (China)
scalability	1000	<50	100s	millions	100s	?	100s-1M

Les Réseaux Quantiques - Pourquoi

- **Communications longue distance** protégées par la distribution de clés quantiques avec des niveaux de confidentialité et de sécurité impossibles à atteindre avec les techniques de cryptage conventionnelles.
- **Des serveurs quantiques dans le Cloud** puissants et sûrs en connectant et en amplifiant les capacités des processeurs quantiques individuels.
- Les réseaux quantiques tireront parti de certaines technologies déjà déployées pour les communications optiques modernes, telles que les lasers, les fibres et les détecteurs.
- Les réseaux quantiques nécessitent des photons uniques - les plus petits éléments constitutifs de la lumière - pour connecter les dispositifs quantiques entre eux.
- Les photons uniques permettent de nombreuses capacités spéciales des réseaux quantiques
- Mais les photons uniques posent un grand défi :
 - La mécanique quantique interdit leur amplification, ce qui limite la portée du réseau.
 - Nécessitent des nouvelles technologies, telles que les répéteurs et les transducteurs quantiques,

Internet Quantique

- Un Internet Quantique est une **interconnexion hétérogène de réseaux quantiques**, c'est-à-dire un réseau de dispositifs quantiques capables:
 - d'échanger des bits quantiques (qubits) et de
 - générer et de distribuer des états quantiques intriqués.
- L'internet quantique repose sur deux concepts fondamentaux :
 - le qubit et l'intrication.
- Le postulat de la mesure a de profondes implications sur la pile de protocoles de l'internet quantique.
- le non-clonage interdit de copier un état quantique inconnu.

Application	
Transport	Qubit transmission
Network	Long distance entanglement
Link	Robust entanglement generation
Physical	Attempt entanglement generation

Thales - TeQuantS

Rattraper la Chine !

- ▶ Thales Alenia Space et ses partenaires signent un contrat avec l'Agence spatiale européenne pour réaliser le projet de communications quantiques par satellite TeQuantS
- ▶ TeQuantS1 vise à développer les technologies de communications quantiques entre l'espace et la Terre.
- ▶ Ce contrat, qui s'inscrit dans le cadre de la composante *4.0 Core Competitiveness* du programme ARTES de l'ESA2, est soutenu par le Centre national d'études spatiales (CNES) et l'Agence spatiale autrichienne.
- ▶ Le projet TeQuantS prévoit le développement des technologies quantiques nécessaires aux applications de cyber sécurité et au développement du futur **réseau Internet Quantique**.
- ▶ Ces technologies permettront à Thales Alenia Space et ses partenaires de réaliser des satellites et stations sol optiques d'ici fin 2026.
- ▶ Le projet TeQuantS contribuera ainsi à démontrer les performances des liens de communications quantiques longue distance par satellite.

Les Capteurs – *Doper l'IoT par la Surpuissance Quantique*

- Maisons intelligentes, voitures autonomes, trains automatisés, contrôle du trafic aérien, industrie 4.0, nouvelles sources d'énergie, dispositifs et services médicaux connectés, systèmes de défense et de sécurité de dernière génération...
- Les capteurs sont de toutes formes et tailles.:
 - De la plus simple **jauge de température utilisée en cuisine** jusqu'aux **radars ultrasophistiqués** utilisés pour surveiller l'espace aérien, les capteurs jouent un rôle prépondérant dans la compréhension par l'homme du monde qui l'entoure.
- Dans un environnement de plus en plus connecté et numérique, les capteurs quantiques augmentent et élargissent les sens humains afin de pouvoir obtenir de nouvelles connaissances.

Les capteurs « quantifiables »

(Thalès)

- **Antennes quantiques:** Les dispositifs supraconducteurs à interférence quantique sont aujourd'hui largement étudiés pour le développement d'antennes quantiques miniatures, capables de couvrir un très large spectre d'ondes, et ainsi offrir un avantage compétitif en particulier lorsqu'il s'agit de capter des basses fréquences
- **Les capteurs quantiques à l'état solide,** tels que les centres colorés dans le diamant, ont démontré leur capacité à mesurer des champs magnétiques de très faible intensité: capteurs biologiques à l'imagerie par résonance magnétique, détection de défauts dans les métaux ;
- **Les capteurs biologiques** Les ions terre-rare vont permettre de caractériser et traiter les signaux radiofréquences ou optiques: désencombrer et optimiser les réseaux – les fréquences étant des ressources rares – et servira également des applications de renseignement dans le domaine de la défense.
- **Instrument de navigation des avions** centrales inertielle quantiques s'appuyant sur la technologie des atomes froids. Passage d'une précision d'atterrissage de quelques kilomètres à une précision d'un mètre
- **Magnétomètres ultrasensibles et miniaturisés** va révolutionner le domaine médical : nouvelle génération d'IRM miniaturisés, études du fonctionnement du cerveau permettant de diagnostiquer les dysfonctionnements cognitifs ou les tumeurs

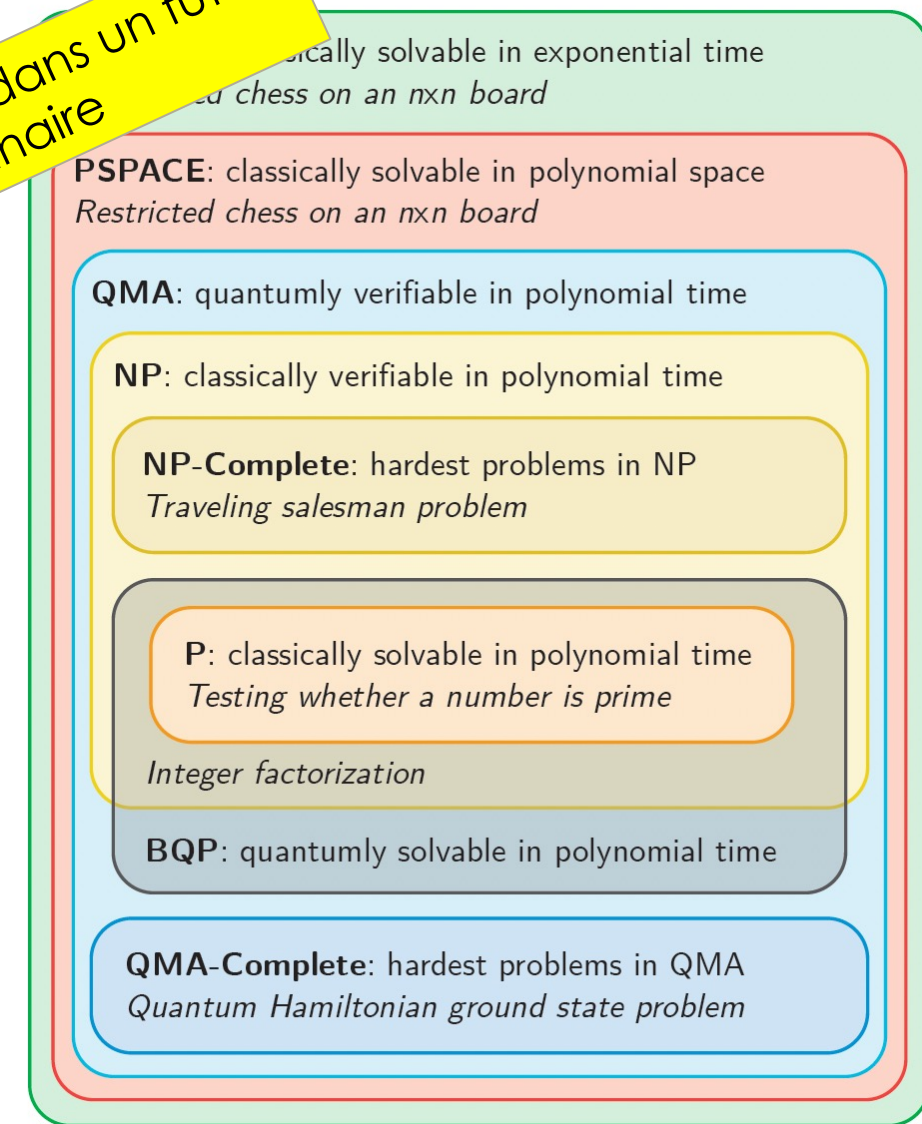
Relevant complexity classes together with a problem examples.

For the chess example, the word "restricted" refers to a polynomial upper bound on the number of moves.

The containment relations are suggestive.

Some of them have not been mathematically proven, being a well-known open problem whether P is equal to NP .

Seront traités dans un futur séminaire

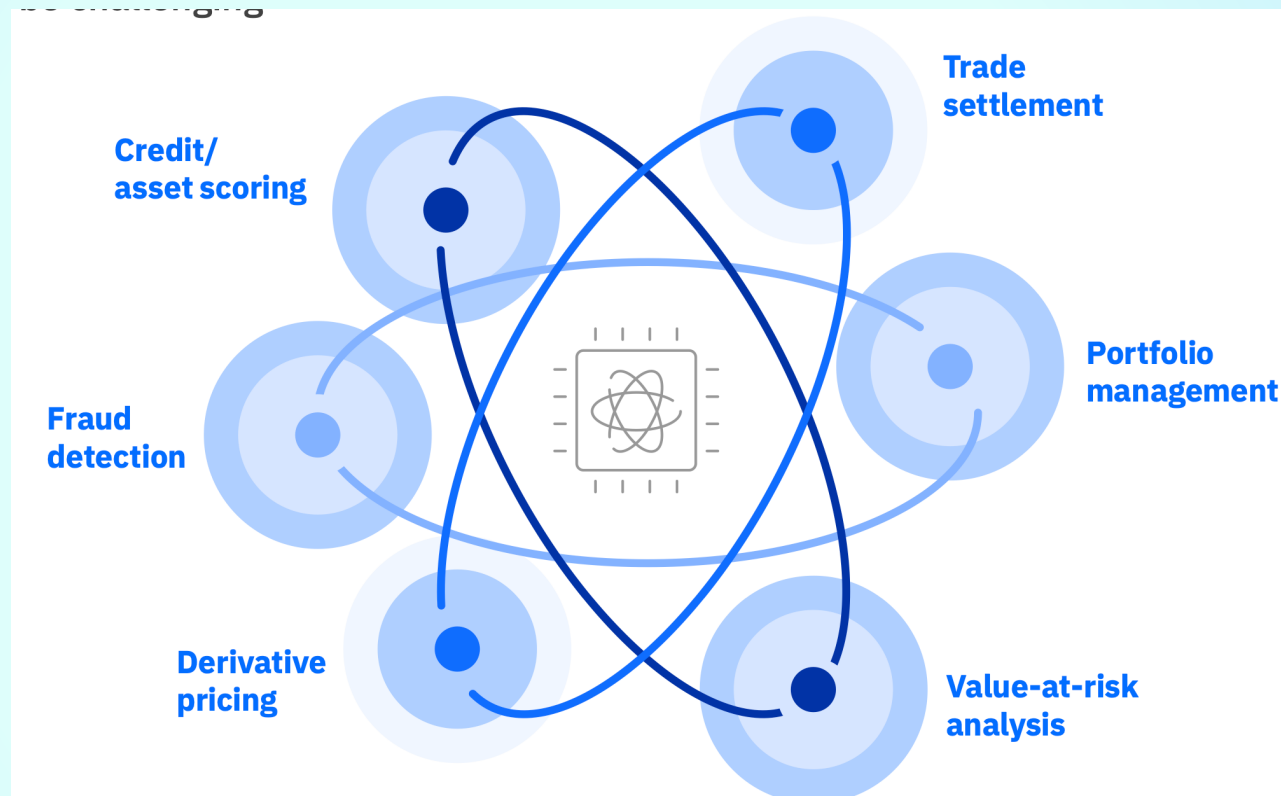


Les Applications – Cas d'Usage

Cas d'usage – Solutions Livrées aux clients – consulter les liens suivants

- <https://www.pasqal.com/customer-story>
- https://www.quandela.com/wp-content/uploads/2023/05/Quandela_Use-Cases.pdf
- <https://www.ibm.com/quantum/business>
- <https://meetiqm.com/products/iqm-co-design/>
- <https://www.dwavesys.com>
- <https://multiversecomputing.com/verticals>

Finance



Banking and Financial Markets

- Le secteur des services financiers a l'habitude d'appliquer avec succès la physique pour résoudre ses problèmes les plus épineux. Le modèle Black-Scholes-Merton, par exemple, utilise le concept de mouvement brownien pour fixer le prix des instruments financiers - comme les options d'achat européennes - au fil du temps.
- L'application de la technologie quantique émergente aux problèmes financiers, en particulier ceux liés à l'incertitude et à l'optimisation sous contrainte, devrait également s'avérer extrêmement avantageuse pour les pionniers. Imaginez que vous puissiez effectuer des calculs qui révèlent des possibilités d'arbitrage plus rentables que les concurrents ne peuvent pas voir. En outre, l'utilisation des données comportementales
- pour améliorer l'engagement des clients et permettre des réactions plus rapides à la volatilité du marché (par exemple, calcul du risque intrajournalier par rapport au risque au jour le jour) sont quelques-uns des avantages spécifiques que nous attendons de l'informatique quantique.
- Bien qu'il faille encore attendre plusieurs années avant de voir des applications commerciales à grande échelle, l'informatique quantique devrait permettre de créer des produits et des services révolutionnaires qui résoudront probablement des problèmes commerciaux très spécifiques d'ici trois à cinq ans.
- Les cas d'utilisation spécifiques de l'informatique quantique pour les banques et les marchés financiers peuvent être classés en trois catégories principales : le ciblage et la prédiction, le profilage des risques et l'optimisation des portefeuilles.

Optimisation – Financial Use Case (JPMorgan)

- Compte tenu de l'abondance des instruments d'investissement, des combinaisons de portefeuilles et des scénarios financiers potentiels, les conseillers financiers d'aujourd'hui ne peuvent pas construire et gérer un portefeuille financier sur mesure ayant évalué la quasi-totalité des options possibles.
- Mais les ordinateurs quantiques pourraient étudier l'univers des options d'investissement, en exécutant des scénarios d'évaluation et de risque adaptés aux critères de performance spécifiques de chaque client.
- JP Morgan Chase, en collaboration avec IBM, expérimente déjà l'informatique quantique à la recherche d'un avantage quantique dans des domaines tels que les stratégies de négociation, l'optimisation des portefeuilles, l'évaluation des actifs et l'analyse des risques.
- Les enjeux sont importants.
- Si une institution financière parvenait à acquérir un avantage concurrentiel grâce à l'informatique quantique, elle pourrait accumuler des milliards pour ses clients et ses actionnaires avant que la concurrence ne soit en mesure de la rattraper.

QML - Quantum Enhanced AI

- Étant donné sa capacité à explorer un large éventail de possibilités qu'un ordinateur classique ne peut pas traiter, l'informatique quantique pourrait étendre les capacités de l'IA.
- En fait, une symbiose entre l'IA et l'informatique quantique commence à engendrer un cycle vertueux de progrès dans les deux domaines.
- Par exemple, les algorithmes quantiques peuvent améliorer l'apprentissage automatique dans le domaine du regroupement de données, tandis que l'apprentissage automatique peut être utilisé pour mieux comprendre les systèmes quantiques
- Les ordinateurs cognitifs quantiques pourraient finir par envahir pratiquement tous les secteurs, offrant aux professionnels une aide à la décision avancée et proactive, aux employés une formation ciblée et réactive, et aux clients des relations avec les fournisseurs adaptées et personnalisées.

IROPS (Irregular Operations) Airlines

- En raison de la portée massive de l'IROPS et de la complexité du problème d'optimisation mathématique globale qui en résulte, la résolution d'une seule perturbation opérationnelle sur les ordinateurs d'aujourd'hui pourrait prendre des années, voire des siècles. En améliorant les algorithmes quantiques et les systèmes de correction d'erreurs, les compagnies aériennes pourraient être en mesure de.. :
- Améliorer la précision et la vitesse des simulations de scénarios qui quantifient l'impact des solutions potentielles sur les vols et les passagers futurs - et le faire à temps pour répondre à une perturbation. Les algorithmes d'informatique quantique se sont déjà révélés efficaces pour choisir les meilleurs scénarios dans les simulations de Monte Carlo utilisées dans le secteur bancaire et financier.
- Fournir un outil de simulation aux analystes des centres de contrôle des opérations afin qu'ils puissent tester des scénarios de manière proactive avant un événement majeur susceptible de perturber les opérations, comme des arrêts de travail des contrôleurs aériens ou des équipages, ou des retards de livraison d'avions. En raison de leur complexité, ces questions ne peuvent aujourd'hui être résolues que pour chaque domaine fonctionnel séparément, ce qui empêche le développement de solutions intégrées.
- Les capacités quantiques pourraient ainsi raccourcir considérablement le temps de rétablissement et réduire le coût des opérations irrégulières, tout en atténuant leur impact négatif sur les passagers.

Chemical and Petroleum

- ▶ The chemical industry has a hand in about 7%—or \$5.7 trillion—of global domestic product, along with approximately 120 million jobs.
- ▶ Developing new chemical products requires expensive and time-consuming lab work. Today, classical simulations of chemistry can help guide lab testing, but the accuracy of calculations decreases as the complexity of molecular interactions increases.
- ▶ When attempting energy calculations in a quantum mechanical system such as large molecules, calculating all the different parameters, including the movement of electrons, becomes intractable on conventional computers.
- ▶ As a result, modeling many industrially important molecules becomes increasingly inexact—or simply too time consuming to wait for an exact solution.

Healthcare

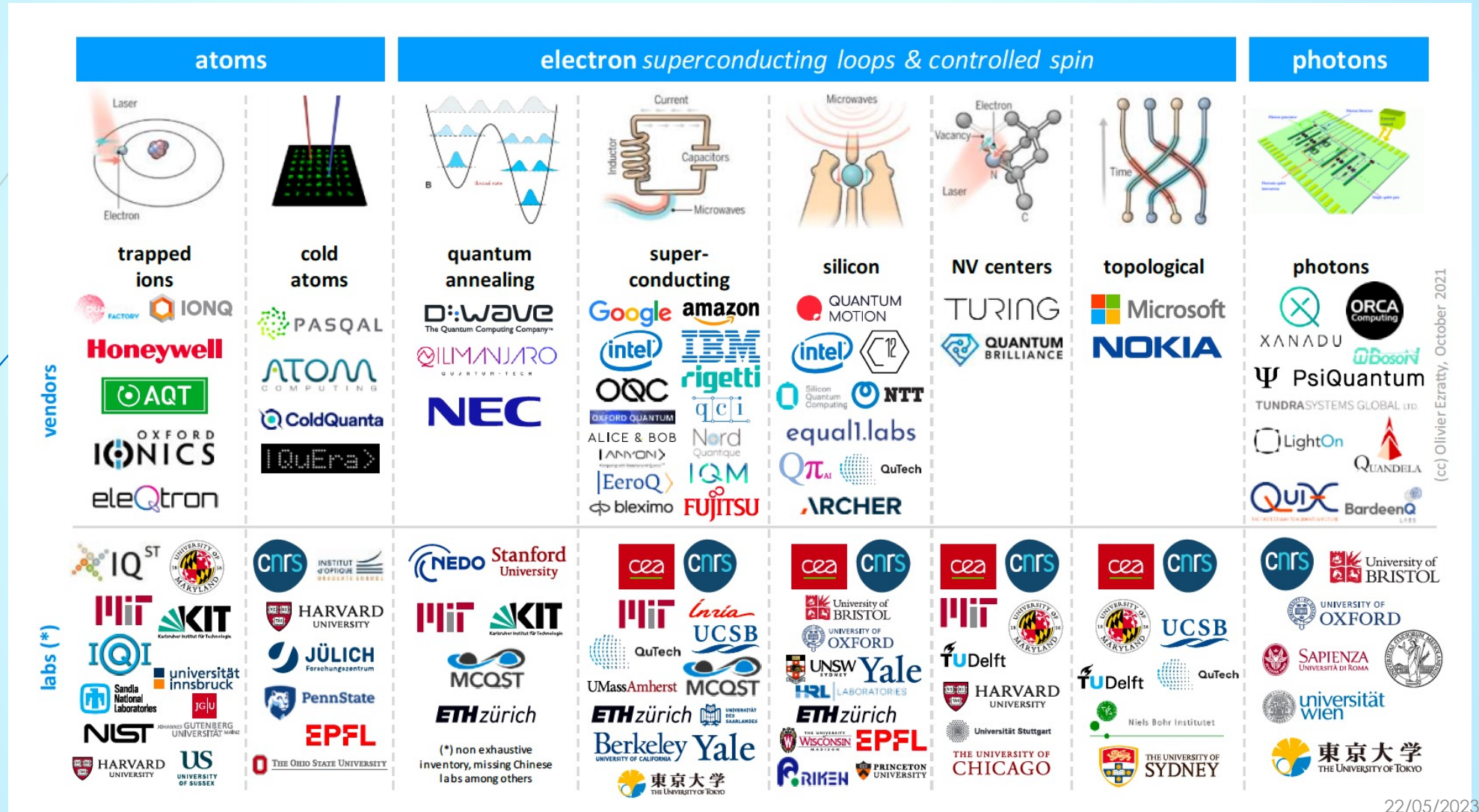
- Les données relatives aux soins de santé, telles que les informations provenant des essais cliniques, des registres de maladies, des dossiers médicaux électroniques (DME) et des dispositifs médicaux, augmentent à un taux de croissance annuel composé de 36 %. De plus en plus, ces données aident à relever les défis associés au "quadruple objectif" des soins de santé : meilleure santé, réduction des coûts, amélioration de l'expérience des patients et amélioration de la vie professionnelle des professionnels de la santé. Dans le même temps, les consommateurs de soins de santé prennent davantage de décisions et doivent naviguer dans un système de plus en plus complexe.
- Des investissements considérables sont réalisés pour fournir les bonnes données et des informations puissantes sur le lieu de soins. Les acteurs historiques du secteur et les nouveaux venus tentent de créer des expériences numériques qui renforcent les comportements sains et préventifs. Malgré cela, la prise en compte des possibilités exponentielles offertes par cette diversité de nouvelles données met à rude épreuve les capacités des systèmes informatiques classiques.
- L'informatique quantique a le potentiel de fournir à la fois plus de puissance de calcul et de vitesse. Cependant, elle nécessite une autre façon de penser, un ensemble de compétences nouvelles et très recherchées, des architectures informatiques distinctes et des stratégies d'entreprise inédites. La technologie a également des implications immédiates en matière de sécurité. La sécurité est un domaine particulièrement important pour les soins de santé, étant donné les responsabilités et les défis du secteur en matière de confidentialité des données.
- Dans les soins de santé, comme dans d'autres secteurs, l'utilisation d'ordinateurs quantiques de concert avec des ordinateurs classiques est susceptible d'apporter des avantages substantiels que l'informatique classique seule ne peut offrir. C'est pourquoi on assiste aujourd'hui à une course aux applications quantiques.
- Trois cas d'utilisation potentiels de l'informatique quantique sont au cœur de la transformation en cours du secteur des soins de santé : l'aide au diagnostic, les primes d'assurance et la tarification, et la médecine de précision.

Life Science

- Dans les sciences de la vie, les principaux défis consistent à comprendre les relations entre la séquence, la structure et la fonction et la manière dont les biopolymères interagissent entre eux, ainsi qu'avec les petites molécules organiques natives de l'organisme ou conçues comme médicaments. Ces problèmes sont complexes sur le plan informatique et sont au cœur de l'analyse génomique, de la conception de médicaments et des prédictions de repliement des protéines.
- C'est pourquoi on assiste aujourd'hui à une course interdisciplinaire vers les applications quantiques. D'ici cinq ans, il est possible que l'informatique quantique soit largement utilisée par de nouvelles catégories de professionnels et de développeurs pour résoudre des problèmes autrefois considérés comme insolubles. Des tendances telles que la généralisation du séquençage efficace à faible coût et l'avènement de l'ère de la "-omics" amènent les entreprises du secteur des sciences de la vie à explorer les moyens de tirer parti de la diversité des nouvelles sources de données. En outre, l'industrie des sciences de la vie est l'une de celles où les gens pourraient le plus directement profiter des futurs avantages de l'informatique quantique.
- L'exploration et la mise en œuvre de cas d'utilisation de l'informatique quantique, associées à de nouveaux progrès scientifiques en matière de matériel et d'algorithmes d'informatique quantique, devraient permettre de passer du potentiel à la réalité au cours des prochaines années. L'informatique quantique a le potentiel de permettre une série de cas d'utilisation perturbateurs dans les sciences de la vie. Il s'agit notamment de
- -La création de thérapies de médecine de précision en reliant les génomes et les résultats -L'amélioration des résultats pour les patients en renforçant l'efficacité de la découverte de médicaments à petites molécules -Le développement de technologies de pointe dans le domaine des sciences de la vie.
- L'amélioration des résultats pour les patients grâce à l'amélioration de l'efficacité de la découverte de médicaments à petites molécules - Le développement de nouveaux produits biologiques basés sur les prédictions de repliement des protéines.

Who's Who

Panorama – Industriels , Labos , Technologies



(cc) Olivier Ezratty, October 2021

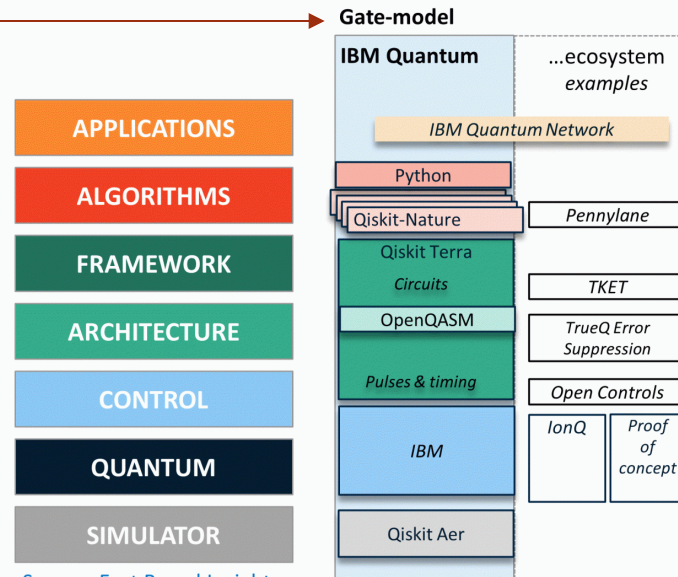
Les Pionniers (HW, SW)

IBM

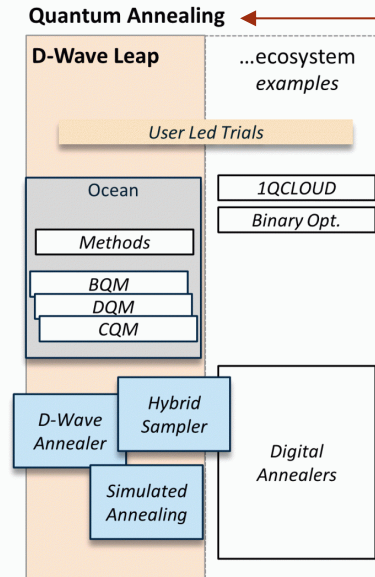
D.Wave

FACT BASED *INSIGHT*

Quantum pioneers



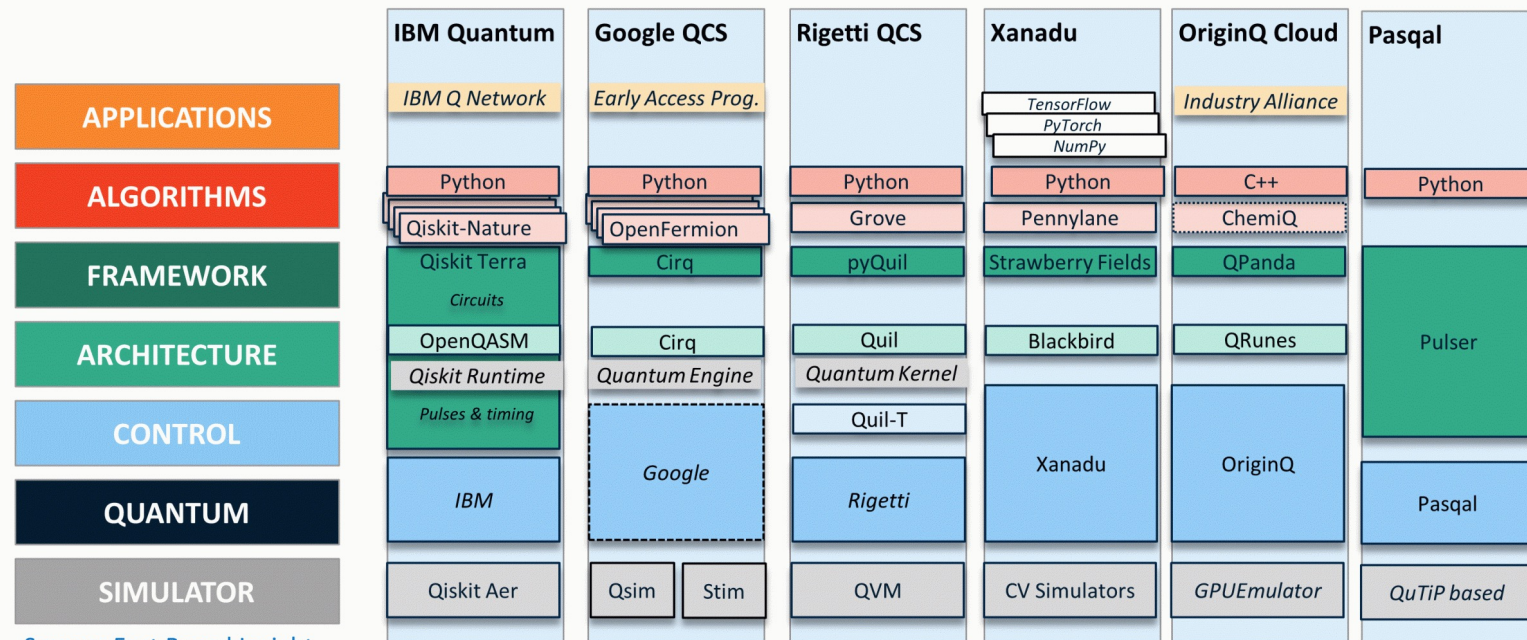
Source: Fact Based Insight



Les Leaders du Modèle Gate-based

FACT BASED *INSIGHT*

Early gate-model full-stack players



Source: Fact Based Insight

Fédérer par le Cloud:

Exemple de Fournisseurs sur Azure

- Quantinuum : système à **ions piégés** offrant des qubits haute fidélité entièrement connectés, de faibles taux d'erreur, la réutilisation des qubits et la possibilité d'effectuer des mesures à mi-circuit.
- IonQ : Ordinateur quantique à **ions piégés** dynamiquement reconfigurable pour un maximum de 11 qubits entièrement connectés, qui vous permet d'exécuter une porte à deux qubits entre n'importe quelles paires.
- Rigetti : Processeurs **supraconducteurs** basés sur la porte qui utilisent la représentation intermédiaire quantique (QIR) pour permettre une faible latence et une exécution parallèle.
- **Microsoft -**
- Pasqal : (**Soon**) processeurs quantiques à base **d'atomes neutres** fonctionnant à température ambiante, avec des *temps de cohérence longs et une connectivité qubit impressionnante*.
- QCI Quantum Circuits, Inc : (**Soon**) circuits **supraconducteurs** à pile complète, avec commentaires en temps réel qui permettent la correction des erreurs et les portes d'intrication indépendantes de l'encodage.

Les Enjeux et Les Investissements

La Course au Leadership – 2017

Comment les USA perçoit le défi ?

*"Let's make no mistake: the competition for a quantum computer is the new arms race. The competition to create the first large-scale quantum computer is heating up. The country that develops one first will have the ability to cripple militaries and topple the global economy...
...To deter such activity, and to ensure our security, the United States must win this new race to the quantum-computer revolution."*

National Review (May 2017)

What quantum computational supremacy means 2019 (Preskill 2019)

“Quantum David vs. Classical Goliath”

It's a programmable **circuit-based** quantum computer. An impressive achievement in experimental physics and a testament to ongoing **progress** in building quantum computing hardware;

We have arguably entered the regime where the **extravagant exponential resources** of the quantum world can be validated.

This confirmation does not surprise (most) physicists, but it's a **milestone** for technology on planet earth.

Building a quantum computer is **merely really, really hard, not ridiculously hard**.

The hardware is working; we can begin a serious search for useful applications.

Ivanka Trump @IvankaTrump
It's official! 🌟 The US has achieved quantum supremacy!
In a collaboration between the Trump Admin, @Google and UC Santa Barbara, quantum computer Sycamore has completed a calculation in 3 min 20 sec that would take about 10,000 years for a classical comp.



5:47 AM · Oct 23, 2019 · Twitter for iPhone

2.1K Retweets 8.9K Likes

Ivanka Trump @IvankaTrump · Oct 23
Replying to @IvankaTrump
#QIS is a critical industry of the future. That's why @POTUS signed the National Quantum Initiative Act into law, supporting robust quantum R&D. We're proud to have contributed to this major milestone, ushering in the next gen of quantum tech in the USA! 🇺🇸

2023 – Comment vaincre la Chine

Trouver un “*Quantum Tsar*”!

The Chinese quantum programme, in contrast, is led by quantum physicist [Jian-Wei Pan](#) and is managed by a tightly co-ordinated group of academic, government and industry partners. The programme is well resourced, with an annual budget estimated to be in the billions of dollars, and has the full support of the Chinese Communist Party. The US’s quantum race with China could be compared in some ways to the race to develop nuclear technology in the 1940s

If the US is going to be successful in surpassing China, it must implement a streamlined, convergent strategy co-ordinated around a technically knowledgeable and programmatically skilled “quantum tsar”.



Where is our Oppenheimer for today’s competition to develop quantum technology?

World Quantum Day (14 Avril): Constat

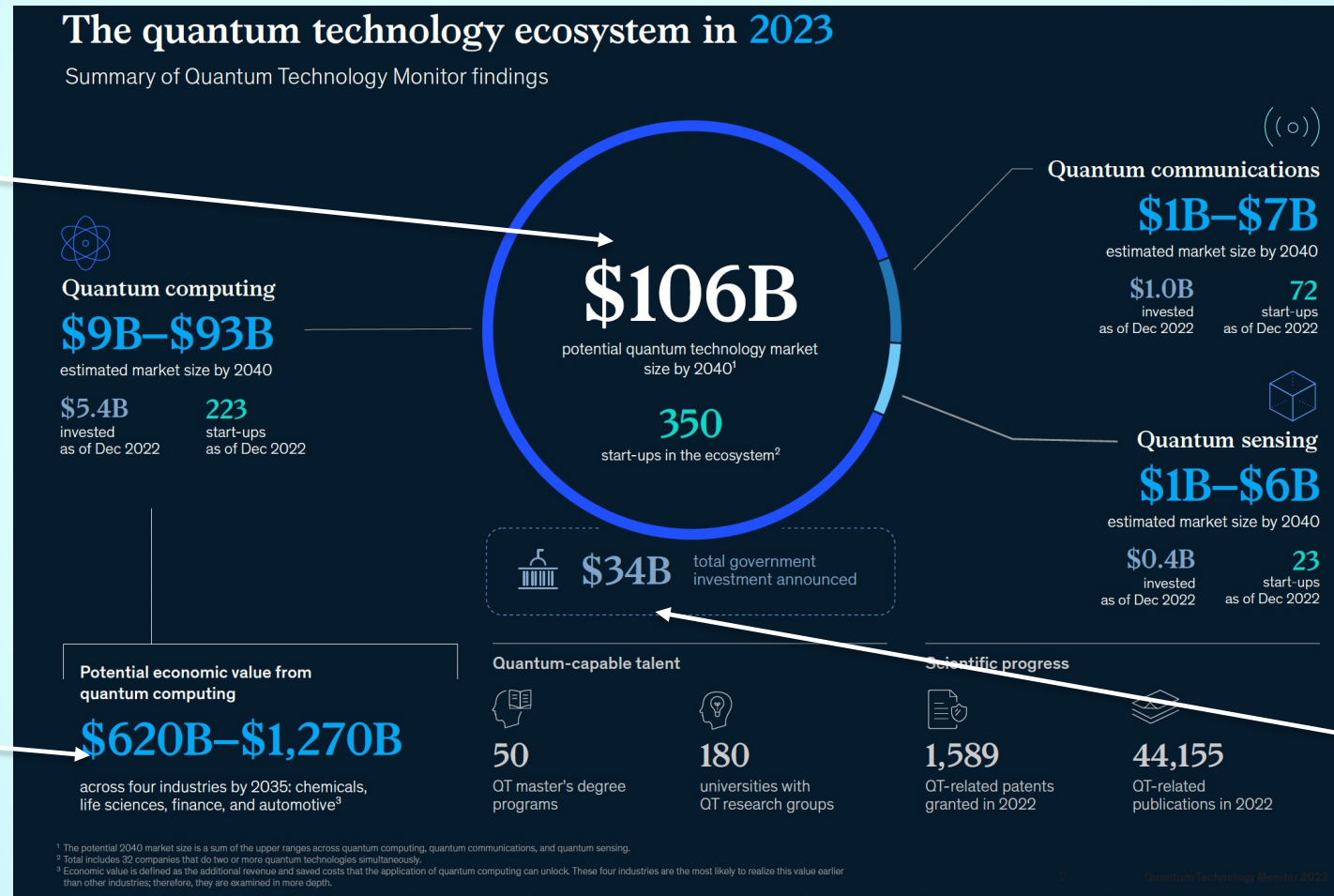
Est-ce que l'Europe peut dépasser les US et la Chine ?

- Les **États-Unis et la Chine** ont toujours fait les **gros titres** en matière *d'innovation et de financement* des technologies **“deeptech”**.
- Les Points forts:
 - Les US sont à la pointe de **Quantum Computing et les Capteurs**
 - La **Chine** réalise des progrès significatifs dans le domaine de la **Communication Quantique**.

McKenzie

Marché potentiel en 2040

Impact en valeur En 2035

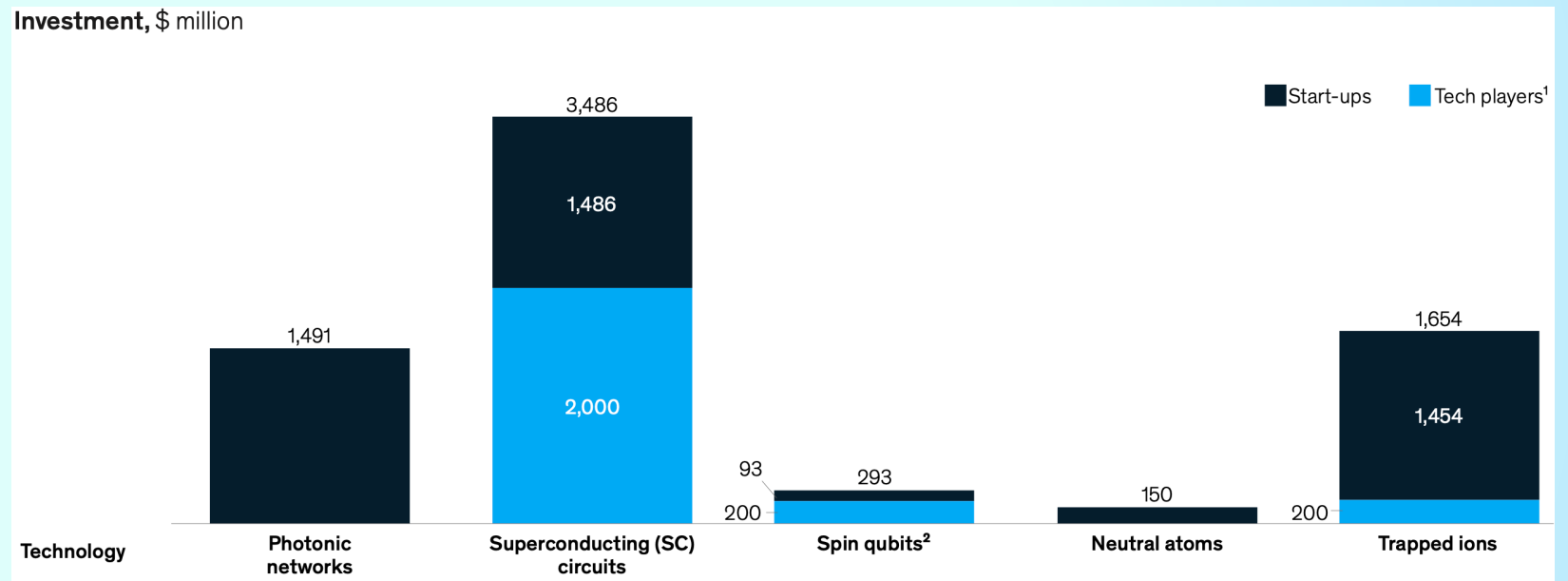


Marché 2040
 Q Compute 9-93 B
 Q Comm 1- 7 B
 Q Sensing 1-6 B

Investissement Gouv. Annoncé

In hardware, Tech incumbents invest most in superconducting circuits, while start-ups invest more in ions and photonic network

Start-up 2022	2022
United States	72 +12
Canada	28 +2
United Kingdom	22 +3
Japan	14 +1
Germany	12 +4
France	11 +3
China ¹	9 +1
Australia	8 +1
Spain	8 +1
Netherlands	7 +1
Finland	6
India	6 +1
Israel	6 +2



France –

Bilan Mars 2023 Plan Quantique

Rappel des Objectifs

- ▶ Dotée d'un financement cumulé de l'Etat d'environ 1 Md€ sur quatre ans, pour un engagement global public-privé de 1,8 Mds€, elle s'articule autour de 6 objectifs stratégiques :
 - Développer les technologies et usages du calcul quantique
 - Maîtriser les technologies de capteurs quantiques
 - Développer et diffuser la cryptographie post quantique
 - Développer les technologies de communications quantiques
 - Maîtriser les technologies habilitantes du quantique
 - Développer les technologies et usages du calcul quantique.



Bilan Mars 2023 Plan Quantique France

Les avancements de la stratégie en quelques chiffres

- 350 millions ont été investis dans le cadre de France 2030
- 150 millions pour financer le Programme de recherche (PEPR) Quantique
- 60 millions en formation dans le cadre de l'appel à manifestation d'intérêt « Compétences et métiers d'avenir »
- 72 millions pour mettre en place une plateforme de calcul quantique hybride
- 80 millions en soutien aux filières industrielles critiques

Pack Quantique Ile de France



9 projets accompagnés-1,9 M€ de soutien régional pour un investissement total de 4 M€

22/05/2023

Plusieurs projets concrets et notables ont émergé en France (liste non exhaustive) :

- **PASQAL**, qui a levé 100 millions d'euros, développe un ordinateur quantique à atomes neutres.
- **Siquance**, issu du CEA et du CNRS, développe et commercialise un ordinateur quantique basée sur les *technologies du semi-conducteur* en capitalisant sur les capacités des producteurs de puce européens.
- **Alice & Bob**, lauréate des concours d'innovation i-PhD et i-Lab de France 2030 travaille à la construction d'un ordinateur quantique universel à correction d'erreur
- **Aqemia**, créée à l'automne 2021, en partenariat avec l'Ecole normale supérieure (ENS) et le CNRS, et spécialisée dans la recherche de médicaments en utilisant l'intelligence artificielle générative et des algorithmes uniques inspirés de la mécanique quantique.

Ecosystème Français - Les Vedettes

C12



Annonces récentes

- OVHcloud commande un machine Quandela
- Eviden /Atos collabore avec les acteurs de soft – ColibriTD, Qubit Pharma ...
- Et avec Pasqal et Quandela pour étoffer sa nouvelle offre Qaptiva

22/05/2023

Conclusions et Références

Le Quantum Computing est livré dès 2022

McKenzie Avril 2023 Quantum Monitor

The year featured comparatively big deals, with four new entrants into the top ten

Exemples de Big Deals

140 à 500 M\$

Top 10 venture capital/private equity investments in QT start-ups of all time, by deal size (descending)

Company	Country	Tech	Segment	Deal size, \$ million	Deal year
SandboxAQ	United States	 ((o)) 	Application software	500	2022
PsiQuantum	United States		Hardware manufacturing	450	2021
IonQ	United States		Hardware manufacturing	350	2021
Rigetti Computing	United States		Hardware manufacturing	345	2022
Arqit	United Kingdom	((o))	Hardware manufacturing	345	2021
IonQ	United States		Hardware manufacturing	300	2021
Quantinuum	United Kingdom		Vertically integrated ¹	300	2021
D-Wave Systems	Canada		Hardware manufacturing	300	2022
PsiQuantum	United States		Hardware manufacturing	230	2020
Origin Quantum	China		Hardware manufacturing	149	2022

22/05/2023

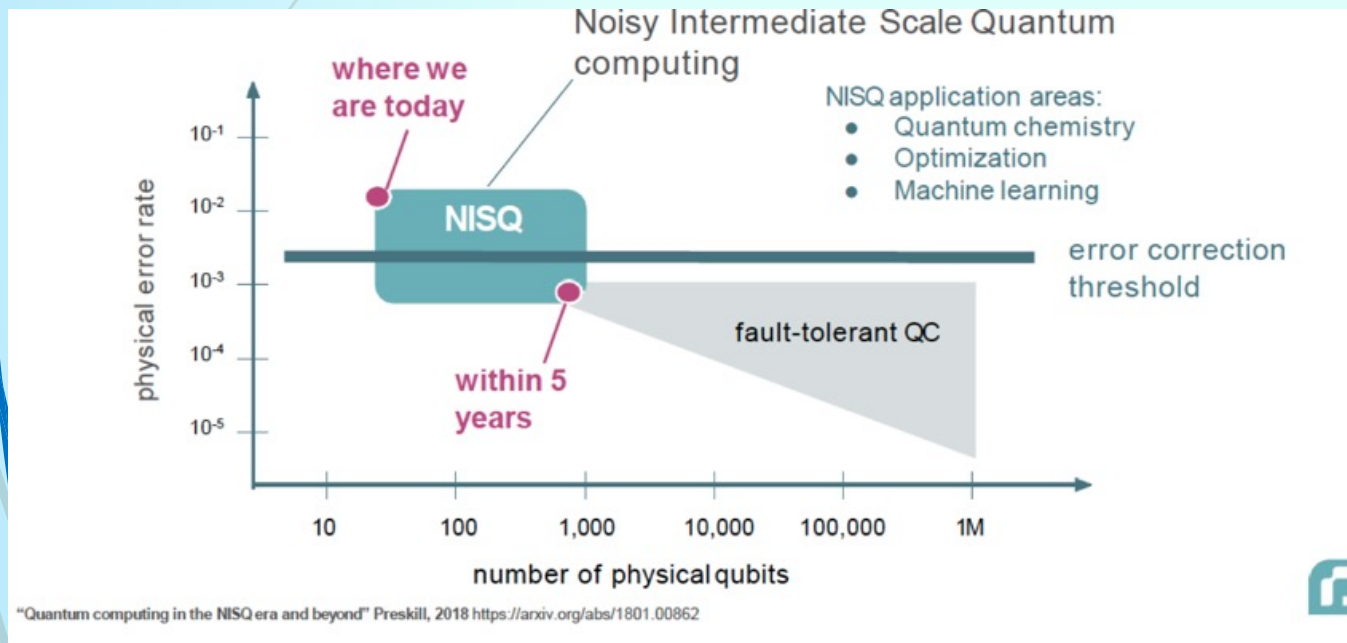
L'Informatique Quantique : est ce Disponible ?

- Les ordinateurs quantiques sont disponibles en 2023 ! MAIS
- Ils sont actuellement très chers et extrêmement difficiles à fabriquer.
- La majorité des machines livrées sont détenues ou exploitées par de grandes entreprises, des instituts de recherche et des organismes gouvernementaux.
- Si vous souhaitez acheter un ordinateur quantique, adressez-vous directement aux fournisseurs : IBM, Rigetti Computing, D-Wave, Google, Pasqal, ou Quandela.
- Ils peuvent offrir un accès à leurs ressources informatiques quantiques à travers le Cloud en mode SAAS
- Le coût d'utilisation de ces services peut varier en fonction du temps et des ressources utilisés, mais il va généralement de quelques Euros à plusieurs milliers d'Euros par heure.

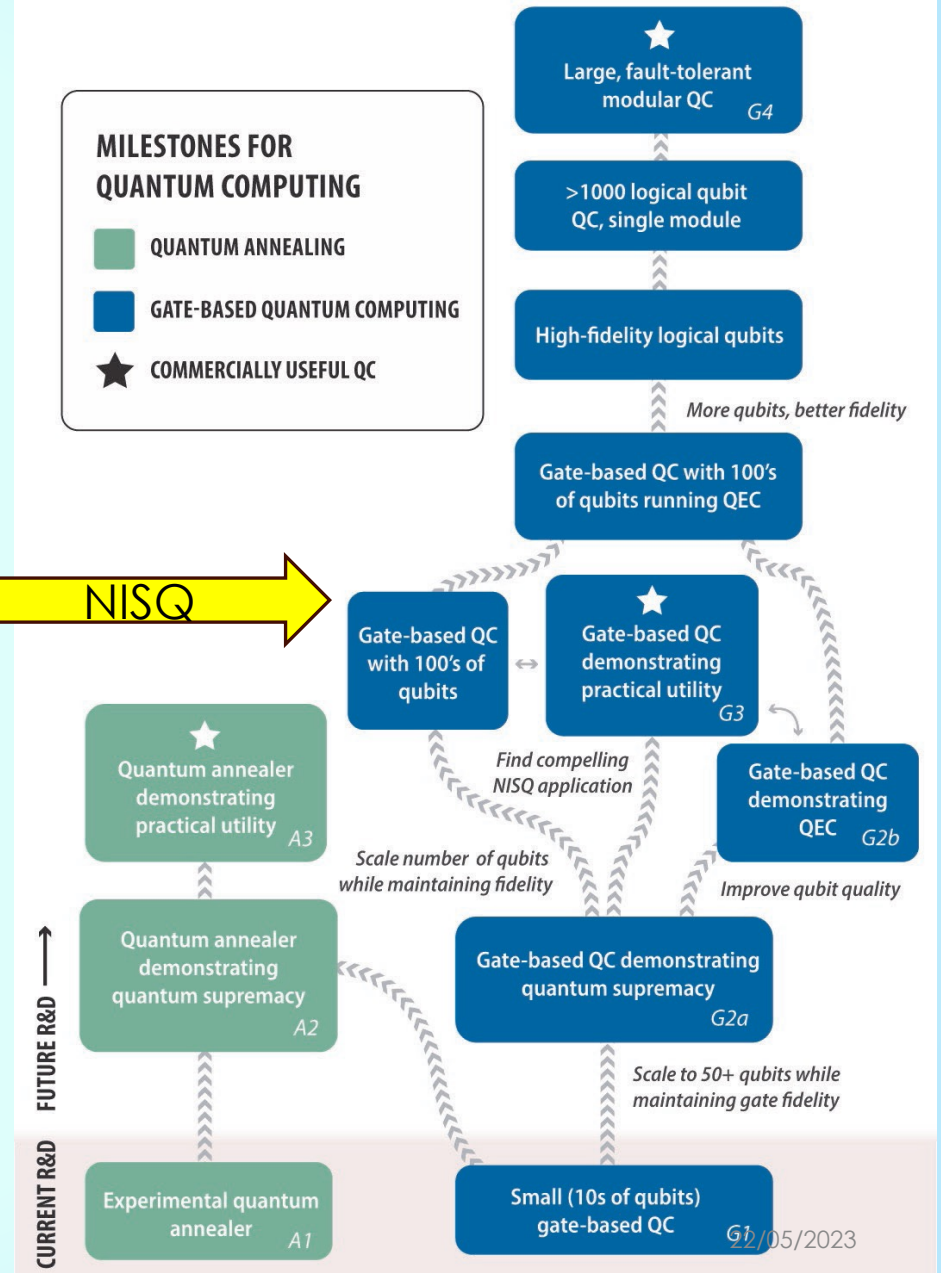
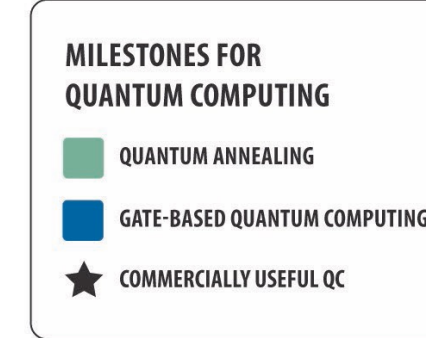
Critères de décision et les Prix en 2023 (selon TQI)

- Points de décision clés : nombre de Qubits et qualité de support du fournisseur.
- Pour les prix, Selon The Verge, l'achat de l'ordinateur quantique D-Wave 2000Q coûterait environ 15 millions de dollars
- Le coût d'achat d'une machine complète à partir de 2023 est actuellement très élevé, le kit qui équipe la plupart des systèmes coûtant des centaines de milliers de dollars.
- Les systèmes quantiques d'IBM sont vendus pour des dizaines de millions dans le cadre d'un contrat de service complet sur plusieurs années.
- Le service d'informatique quantique dans le Cloud Azure de Microsoft offre aux nouveaux utilisateurs 500 dollars de crédits Azure Quantum gratuits à utiliser avec chaque fournisseur de matériel quantique connecté à Azure (voir slide - Exemple de fournisseur de Cloud)
- AWS, les plans tarifaires pour l'utilisation de son service basé sur l'informatique en nuage commencent à 29 dollars par mois et comprennent l'assistance AWS.

Nous sommes dans la Phase NISQ avec ...du Noise et <1000 Qubits



NISQ



Selon Preskill 2018

- **Now, for the first time in human history**, we are acquiring and perfecting the tools to build and precisely control very complex, highly entangled quantum states of many particles, states so complex that we can't simulate them with our best digital computers
- This emerging capability will open the door to **new discoveries**.
- Our confidence that exploration of the entanglement frontier will be rewarding rests largely on two principles:
 - **Quantum complexity** (our basis for thinking that quantum computing is powerful), and
 - **Quantum error correction** (our basis for thinking that quantum computers are scalable to large devices solving hard problems)