

Pourquoi a-t-on besoin d'un ordinateur quantique ?

Frédéric Magniez

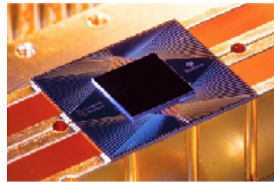


Accueil LI Informatique – 5 septembre 2022



Le buzz quantique

Supr matie quantique



2019-2021

Strat gie nationale



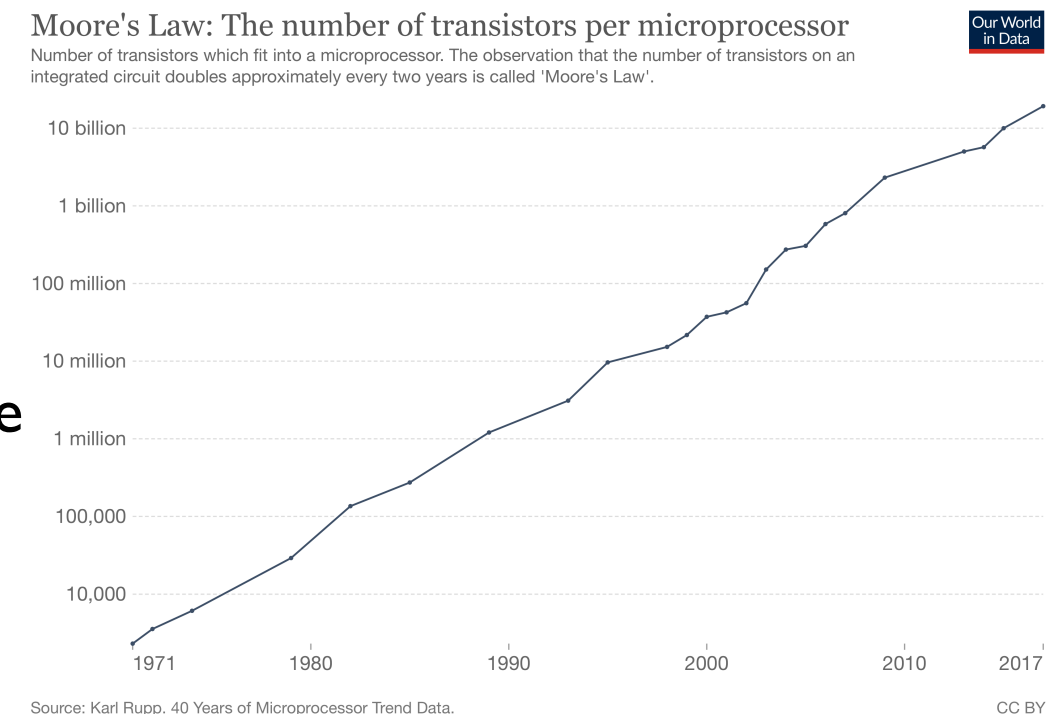
4 janvier 2022

Accélération matérielle

Augmentation des ressources

- ─ Vitesse du processeur
- ─ Miniaturisation
- ─ Temps d'accès à la mémoire interne/externe
- ─ Quantité de mémoire

→ Algorithmes inchangés



Nouvelles technologies

- ─ Multi-processeurs
- ─ Machines mises en réseau
- ─ Cartes GPU, super calculateurs
- ─ Communications rapides

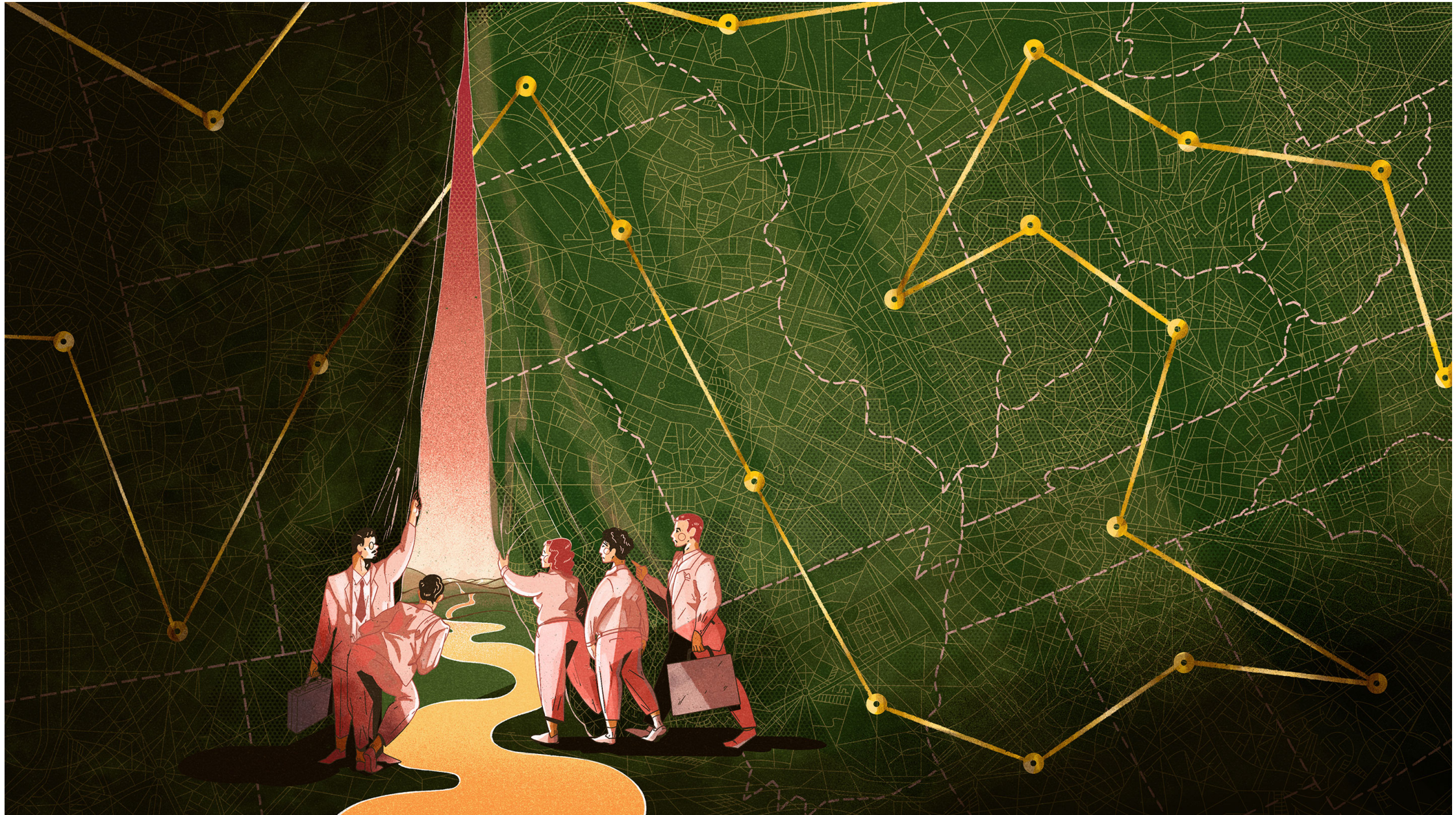


→ Algorithmes revisités

Nouvelles contraintes

- ─ Systèmes complexes
- ─ Données massives, distribuées, bruitées
- ─ Temps réel
- ─ Résultat prouvé

Accélération algorithmique



<https://www.quantamagazine.org/computer-scientists-break-traveling-salesperson-record-20201008/>

→ Matériel inchangé

Simulation par ordinateur



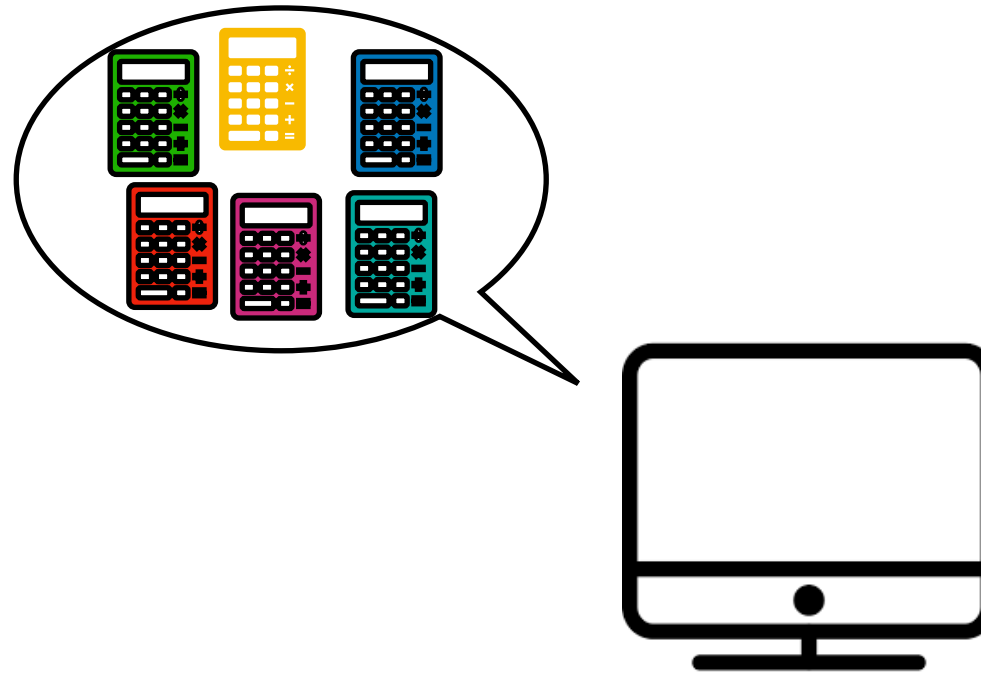
Richard Feynman

**Can quantum systems be simulated
by a classical computer? - 1981**

Une recherche d'abord fondamentale



Alan Turing



Thèse de Church-Turing (calculabilité)

Ce qui est calculable est indépendant des machines actuelles et futures



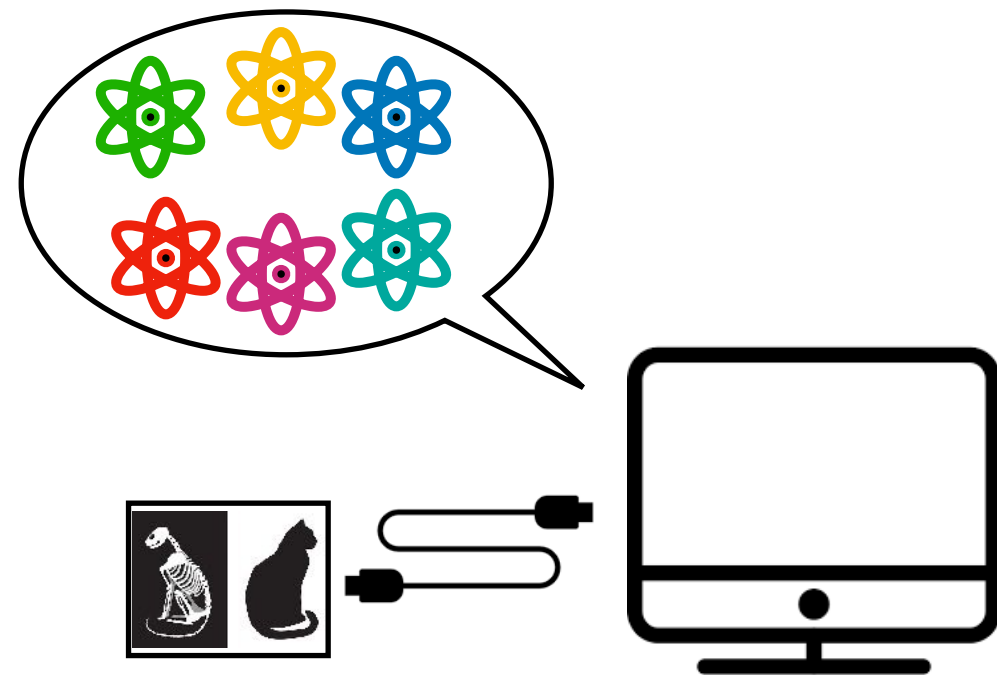
Thèse *moderne* (complexité)

Les progrès technologiques apportent au mieux des gains polynomiaux dans les ressources utilisées (temps, mémoire, processeurs, ...)

Etape I : Ordinateur quantique universel

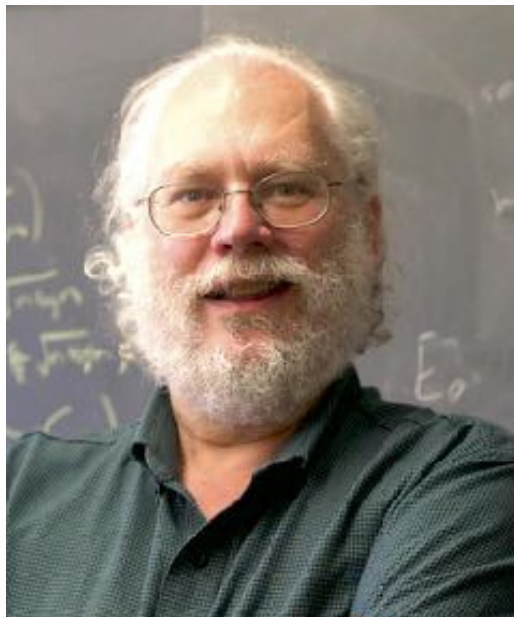


David Deutsch - 1985

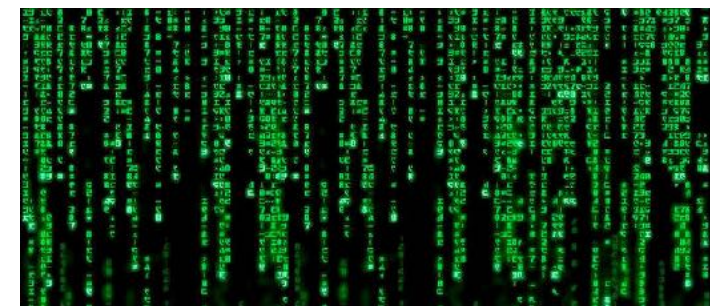
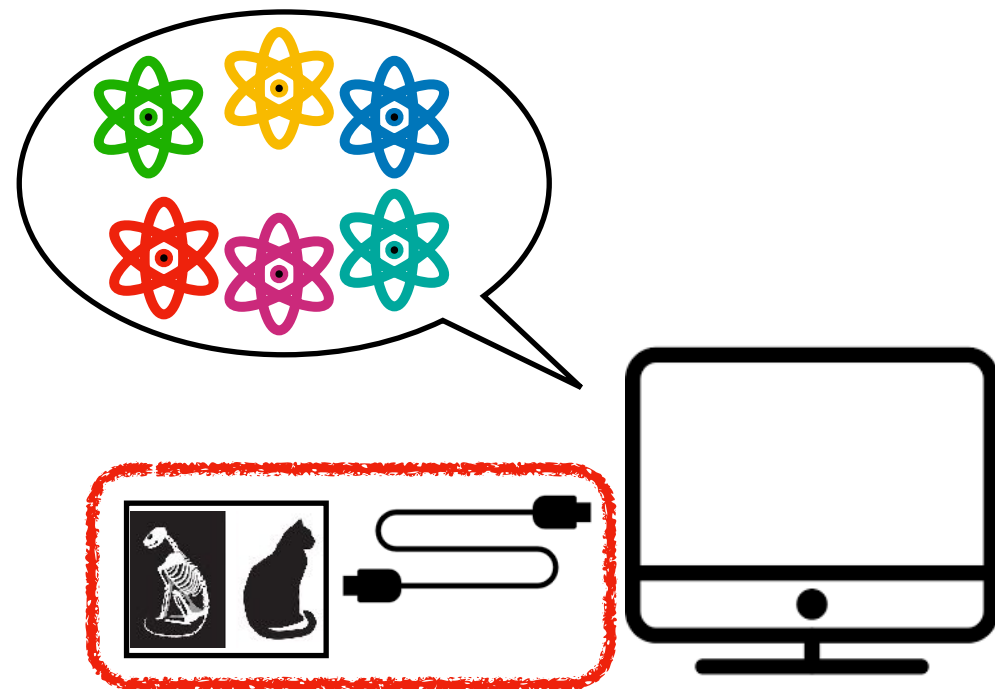


[1993] : Ordinateur quantique universel ET efficace

Etape 2 : Ordinateur robuste aux erreurs



Peter Shor - 1995



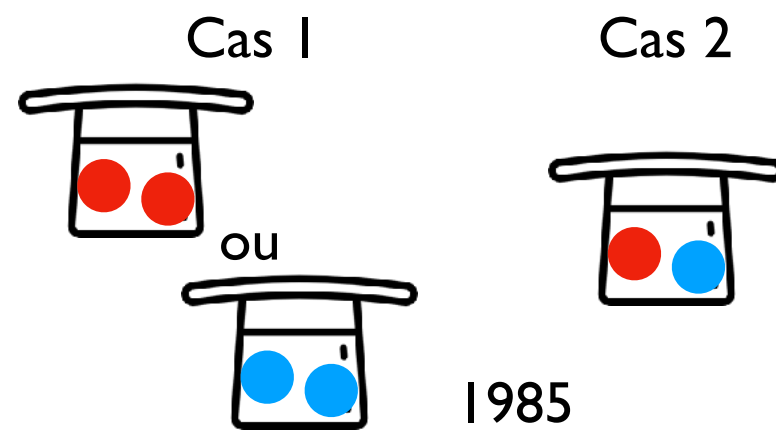
[1998] : En dessous d'un seuil d'erreur, les erreurs ne s'additionnent plus
Mais augmentation des ressources (facteur polylogarithmique)

[2021] : Facteur constant

Défis actuels

- Diminuer le taux d'erreur des prototypes quantiques
- Améliorer la taille des codes correcteurs quantiques

Etape 3 : Des algorithmes (sans ordinateur)



1996 - ...

$$\begin{cases} 2x + 3x - z = 6 \\ x - z + 7z = 4 \\ -x + 2z + 3z = 2 \end{cases}$$

2009 - ...

QUANTUM



~~1940~~ 1994 - ...



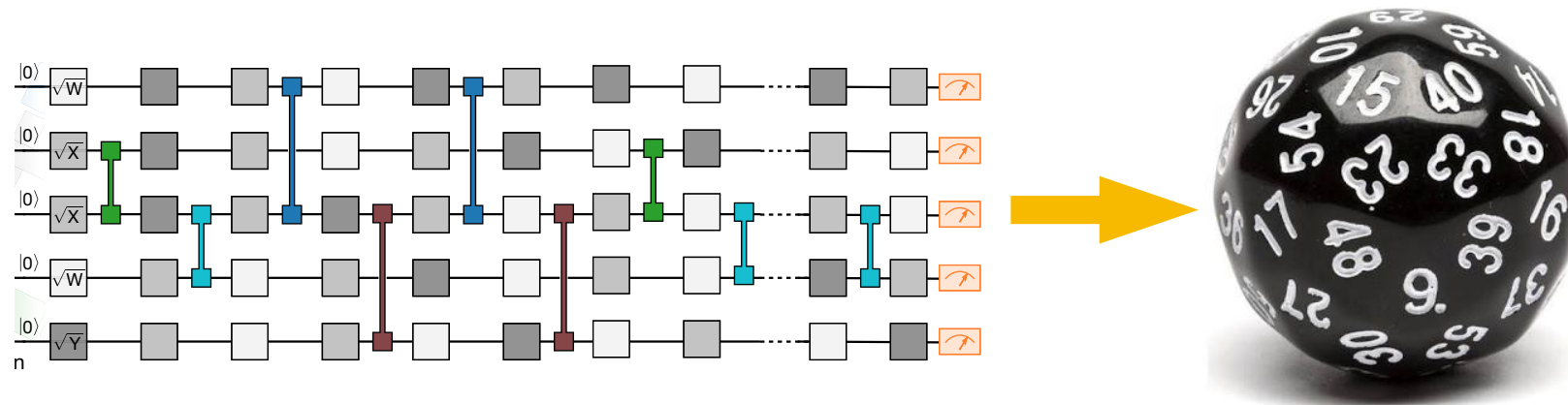
2013 - ...

La vérité...

Supr matie quantique

L'exp rience de Google 2019 puis de USTC 2021

- ─ Choisir un circuit au hasard
- ─ Produire une s quence de valeurs distribu es selon les sorties du circuit



Utilit  ?

Difficult 

- ─ Plusieurs milliers d'ann es sur nos ordinateurs d s 50 qubits
- ─ Instantan  pour la machine quantique de Google / USTC
- ─ MAIS

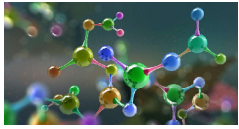
Difficile   v rifier

Avec des imperfections : plus facile   r aliser avec nos ordinateurs

Supr matie n cessite 70-80 qubits ou une meilleure pr cision

Principaux algorithmes

Physique



- Simulation de systèmes quantiques : accélération **exponentielle**

Informatique



- Problèmes artificiels mais fondamentaux : accélération **exponentielle**
- Arithmétique, algèbre : accélération **exponentielle**

Attaques cryptographiques



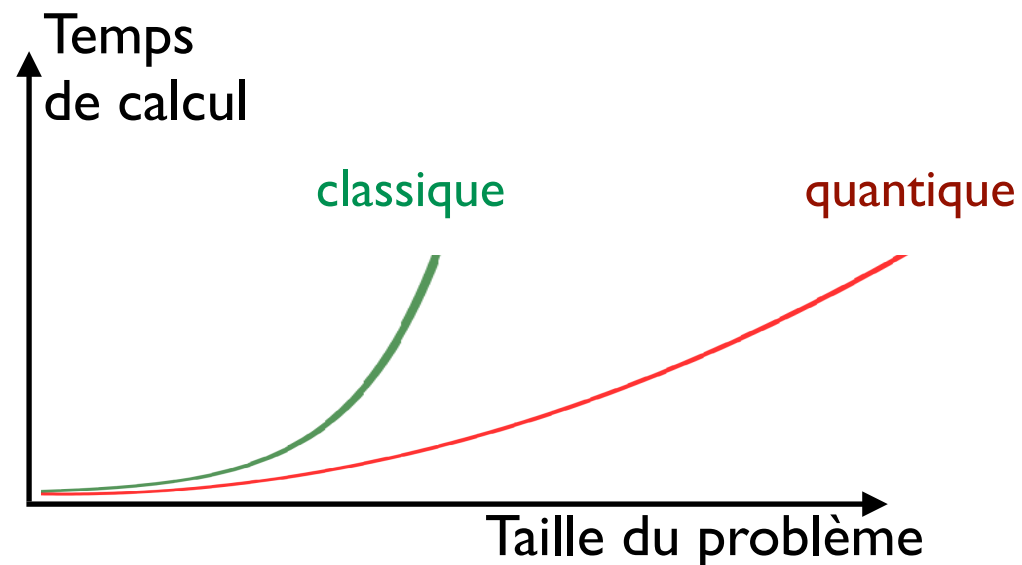
- Aide à la décision, optimisation : **accélération polynomiale**
Recherche opérationnelle



- Algèbre linéaire : accélération **potentiellement exponentielle**
Machine learning, résolution d'équations différentielles

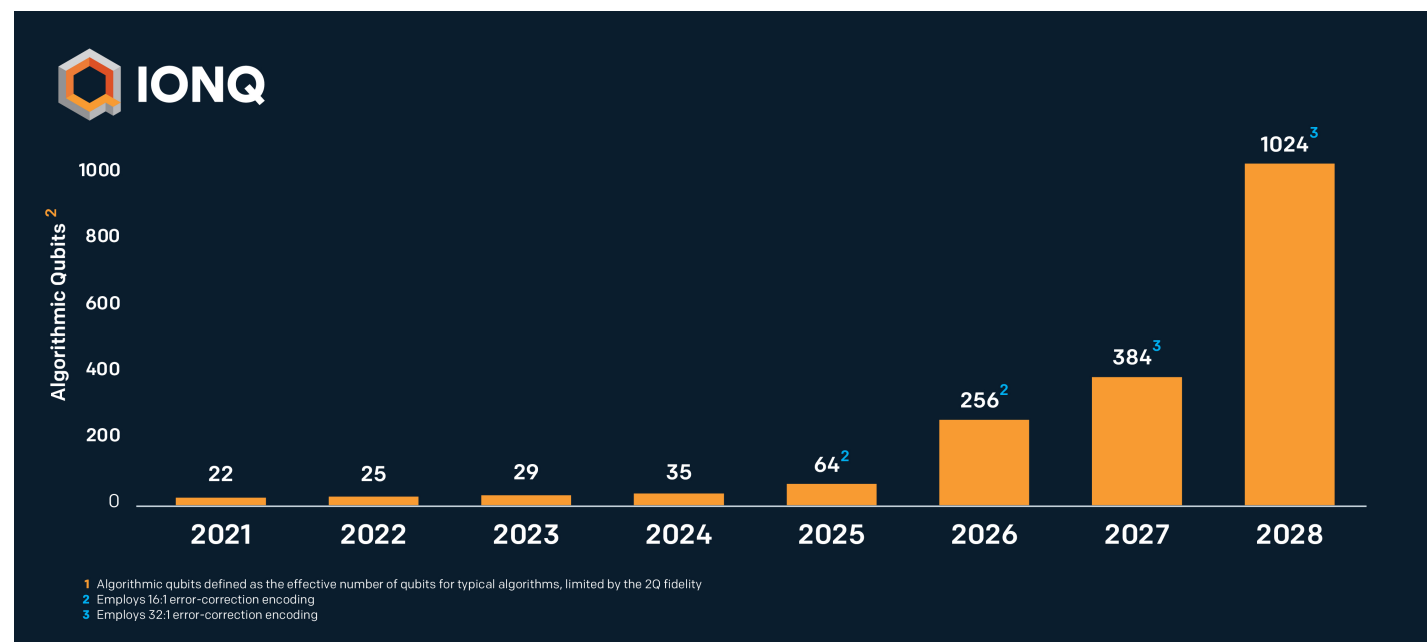
À quand l'accélération ?

Accélération asymptotique



Limitations actuelles

- ─ Mémoire trop petite
- ─ Temps de calcul disponible trop court



Quels usages en attendant ?



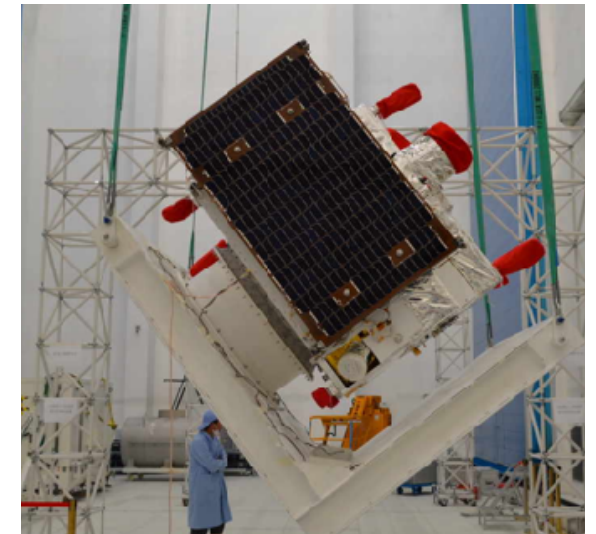
1 bit quantique

- Chiffrement quantique



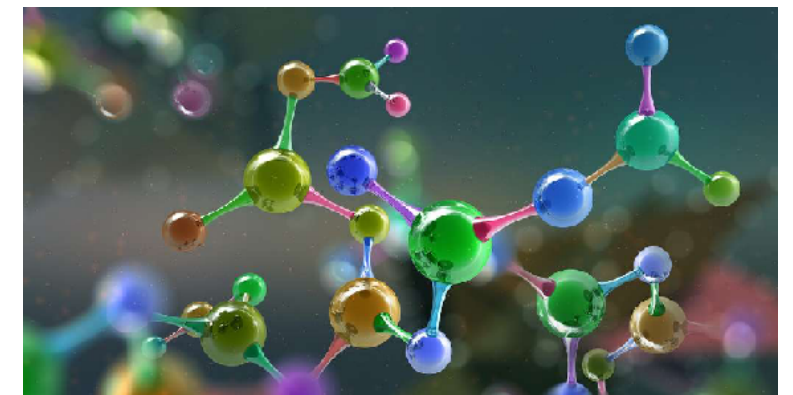
Quelques bits quantiques

- Internet quantique



Super ordinateur augmenté

- Suprémie quantique
- Simulation quantique ?



Quelques millions à milliards

- Ordinateur complet



Les jeux quantiques

Jeux à arbitre

Contexte

- 1 arbitre
- 2 joueurs : A(lice) et B(ob)

Jeu

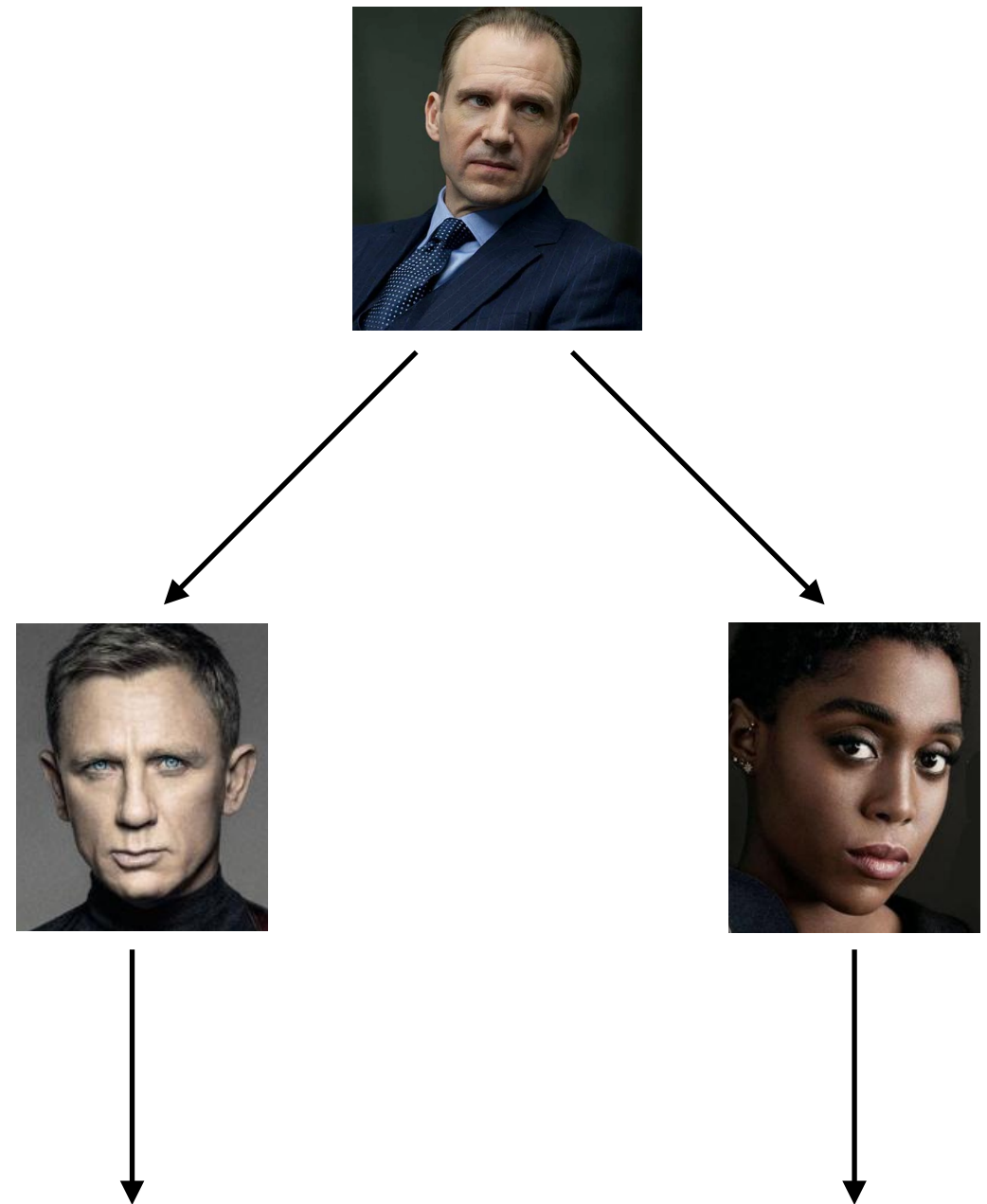
- Un ensemble de challenges est défini
- R en sélectionne un au hasard
- A et B répondent séparément
(stratégie déterminée à l'avance)

Objectif

- Maximiser
 $p = \Pr(A \text{ \& } B \text{ gagnent})$

Exemple

- Répondre la même valeur / une valeur différente



Jeux à arbitre

Contexte

- 1 arbitre
- 2 joueurs : A(lice) et B(ob)

Jeu

- Challenge : Satisfaire $\Phi(x, y, a, b)$
- R envoie $x \rightarrow A$ et $y \rightarrow B$ aléatoires
- A et B répondent $A \rightarrow a$ et $B \rightarrow b$

Objectif

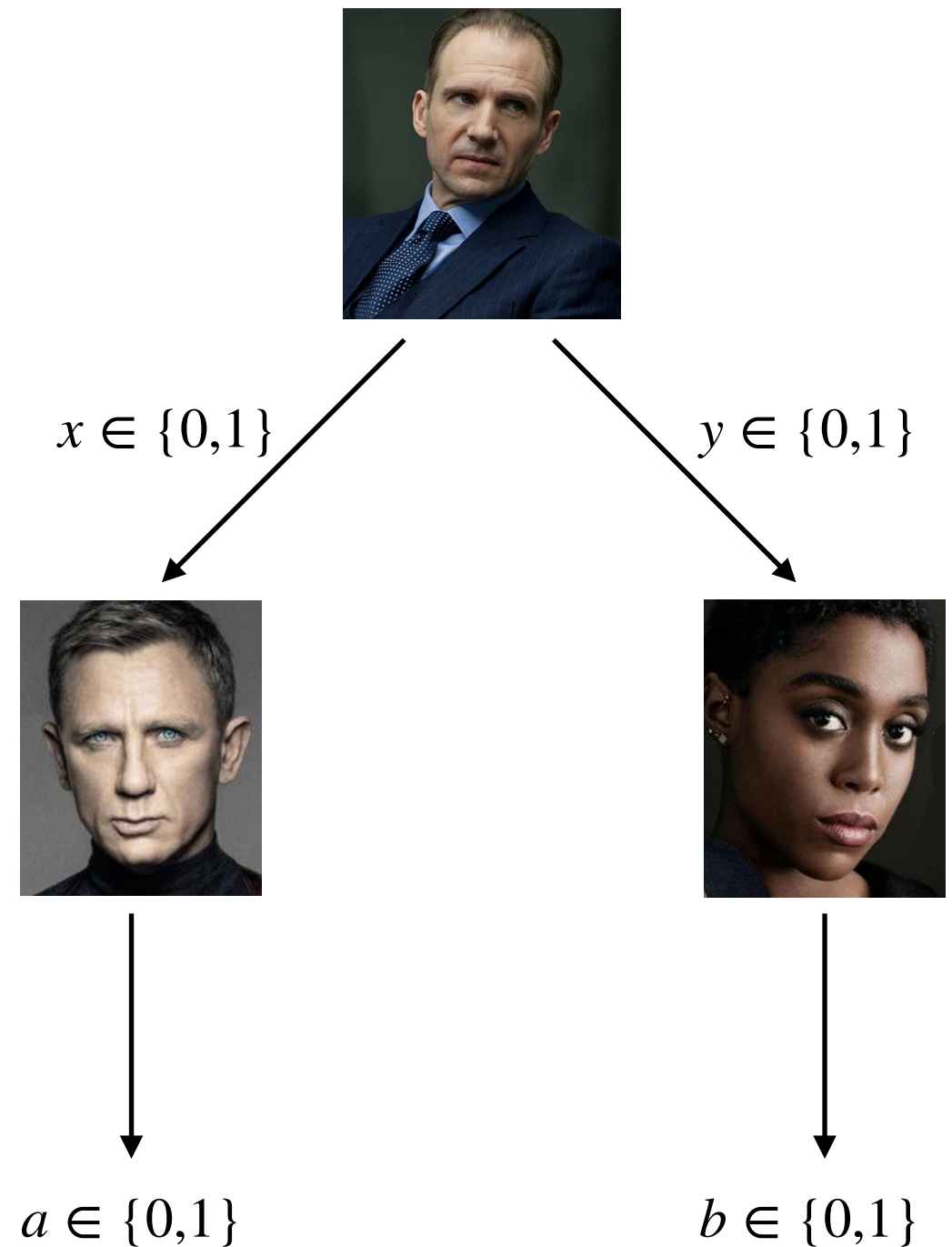
- Maximiser

$$p = \Pr(\Phi(x, y, a, b) \text{ satisfait})$$

Jeu CHSH

- $\Phi(x, y, a, b) : a \oplus b = x \wedge y$

$p = 3/4$ est possible. Peut on faire mieux ?



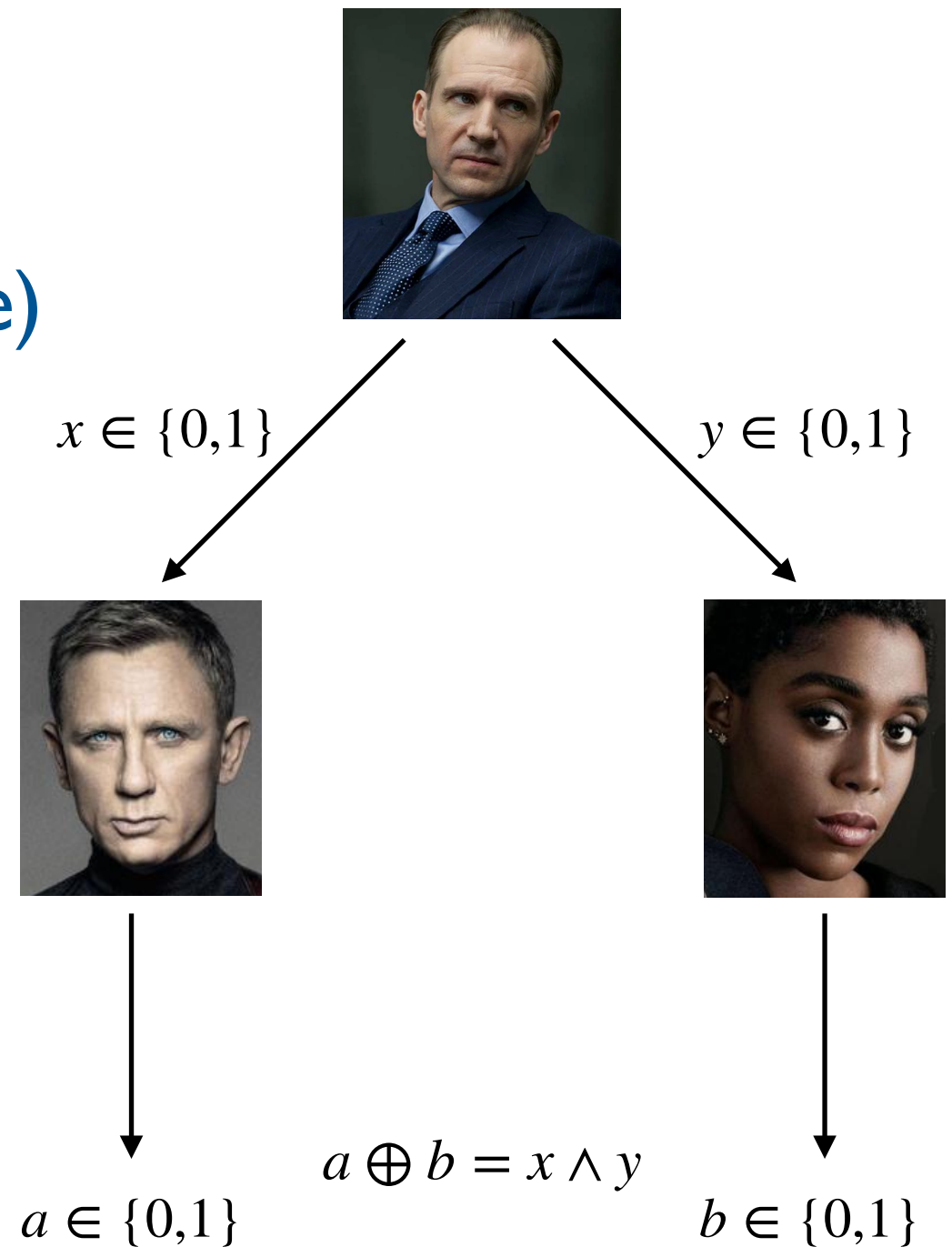
Inégalité de CHSH / Bell

Théorème

- Toute stratégie (classique)
satisfait $p \leq 3/4$

Preuve (stratégie déterministe)

- Modélisation
Réponse de A : $a(x)$
Réponse de B : $b(y)$
- Par l'absurde, si toujours gagnant
Lorsque $xy \neq 11$
 $b(1) = a(0) = b(0) = a(1)$
Lorsque $xy = 11$
 $b(1) \neq a(1)$
IMPOSSIBLE, donc $p < 1$
- Donc $p \leq 3/4$



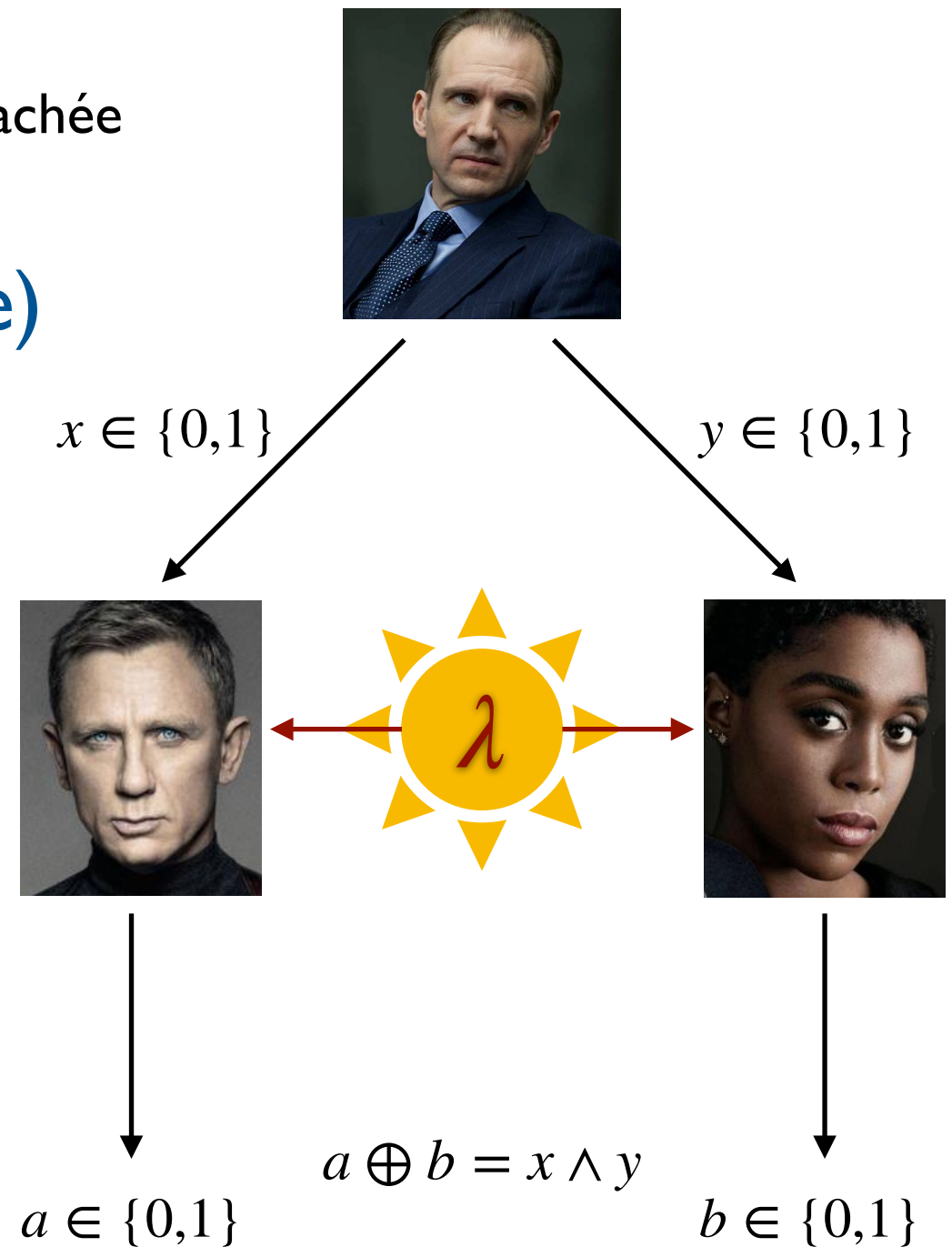
Cas des variables cachées

Théorème

- Toute stratégie (classique) à variable cachée satisfait $p \leq 3/4$

Preuve (stratégie déterministe)

- Modélisation
 λ : variable partagée
indépendante des questions
Réponse de A : $a(x, \lambda)$
Réponse de B : $b(y, \lambda)$
- Pour chaque $\lambda : p_\lambda \leq 3/4$
- Donc $p \leq 3/4$
- Idem pour stratégie probabiliste !



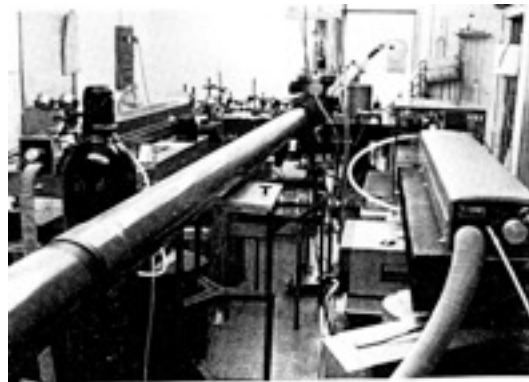
Cas quantique

Théorème

- Il existe une stratégie quantique qui satisfait $p = \cos^2(\frac{\pi}{8}) \approx 0,854$

Réalisation

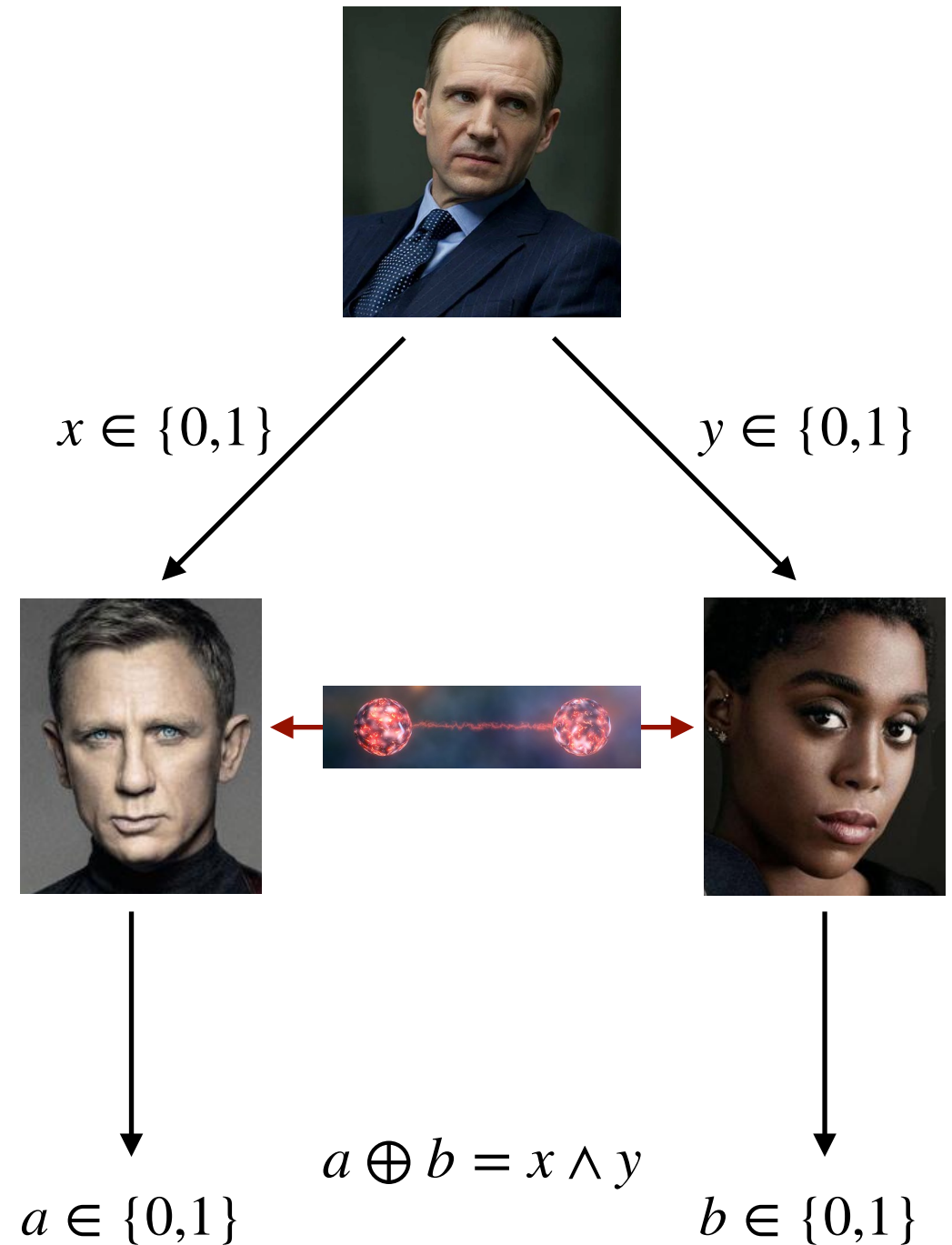
- Expérience à Orsay en 1980-82 d'Aspect-Grangier-Roger-Dalibard



- Aujourd'hui : TP de Master

Conclusion

- Le monde n'est pas classique ! Mais peut être quantique...
- Utilité : Certification d'aléa, de dispositifs quantiques, crypto quantique



Corrélation $\neq$ Communication

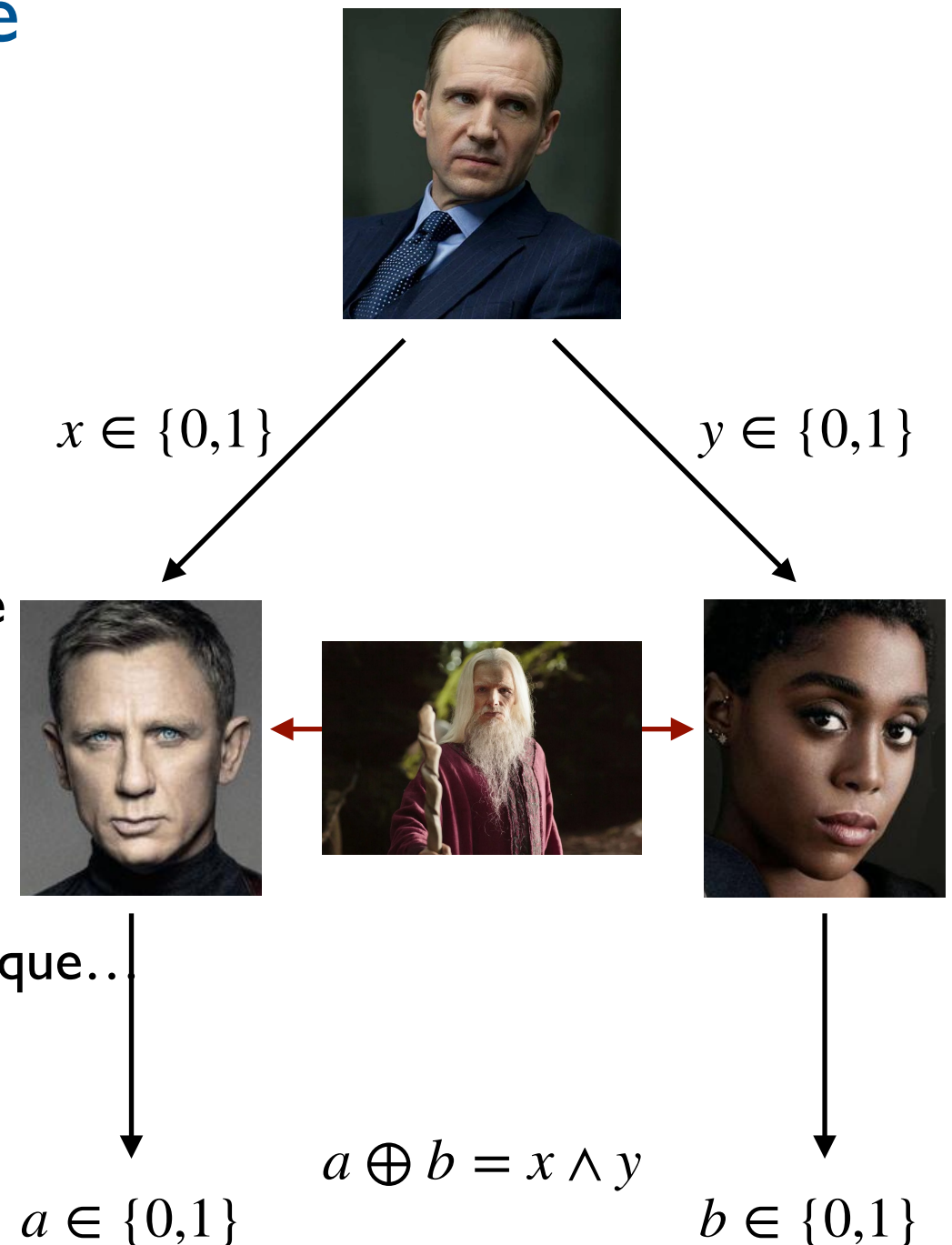
Corrélation toujours gagnante

- Produire a et b séparément aléatoires
- Mais corrélés par

$$a \oplus b = x \wedge y$$

Est-ce possible ?

- Compatible avec la relativité restreinte
Pas de transmission d'information
- En physique quantique
Non : $p \leq \cos^2(\frac{\pi}{8})$
- Peut être dans une autre théorie physique..



Conclusion

Retour en arrière

La France pionnière

- Physique
 - Série d'expériences du groupe d'Aspect, 1980-82
 - Prix Nobel à Serge Haroche, 2012
- Informatique
 - Création du premier groupe autour de Miklos Santha, 1994
- Succès construit sur
 - Une recherche fondamentale
 - Des recrutements et des moyens



Alain Aspect



Serge Haroche



Miklos Santha

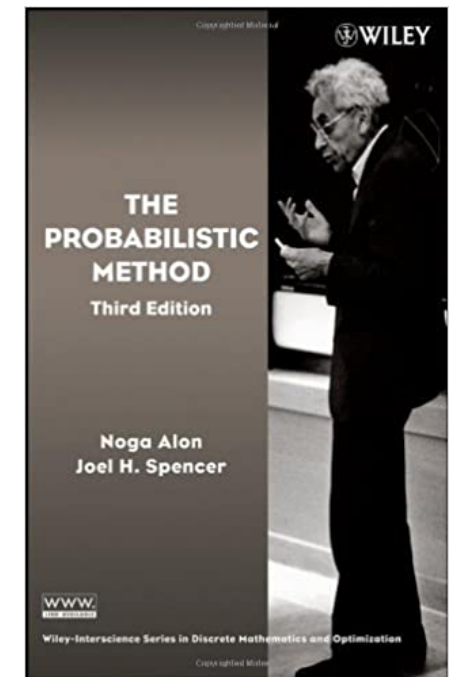
Recherche fondamentale non prévisible

- Mais néanmoins surprenante... et dépassant souvent nos attentes
- Tous ces efforts déboucheront vers de grandes découvertes

Une nouvelle façon de penser

Preuve/méthode quantique

- Analogue des nombres complexes en trigonométrie, analyse...
Exemple : $\cos(x + y) = \cos x \cos y - \sin x \sin y$
- Ou encore de la méthode probabiliste initiée par Paul Erdős
Exemple : Tout graphe a une coupe d'au moins 50%



Des conjectures résolues

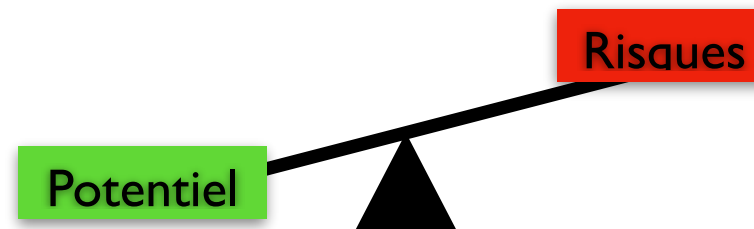
- 2012 : Résolution d'une conjecture de 1988 de Mihalis Yannakakis
liée à la difficulté algorithmique du voyageur de commerce
- 2020 : Réfutation d'une conjecture de 1976 d'Alain Connes
liée aux algèbres de von Neumann

Algorithmes déquantisés

- 2017 : Systèmes de recommandation quantique
- 2019 : Déquantization de l'algorithme

Industrialisation et formation

Enjeux stratégiques



Occasion unique

- Effort technologique historique
- Des algorithmes quantiques par dizaines et bientôt centaines

Quand les deux vont-ils se rejoindre ?

- Frénésie stimulante mais parfois hors de contrôle

Apprendre en programmant

- IBM : <https://quantum-computing.ibm.com>
- Qiskit : <https://qiskit.org/textbook/>