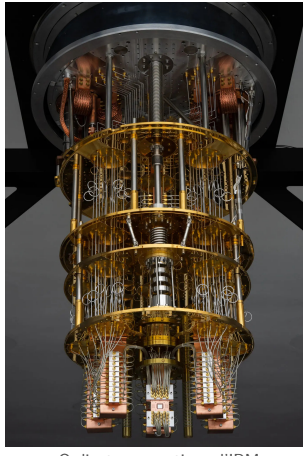
L'ordinateur quantique

Pourquoi et comment ?



Ordinateur quantique d'IBM
James Estrin/The New York Times

Antoine Tilloy
14 Février 2024
Université permanente de Nantes

MINES PARIS | PSL | erc

2019 : annonce par Google de la suprématie quantique

Pour un calcul certes *absolument inutile*

- Sycamore : 200 secondes
- Frontier : 100 000 ans

Frontier

Sycamore

Google est allé un peu vite...

PHYSICAL REVIEW X **10,** 041038 (2020)

Featured in Physics

What Limits the Simulation of Quantum Computers?

Yiqing Zhou,[1,2] E. Miles Stoudenmire,[2] and Xavier Waintal[3]

[1]*Department of Physics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801, USA*
[2]*Center for Computational Quantum Physics, Flatiron Institute, New York, New York 10010, USA*
[3]*Univ. Grenoble Alpes, CEA, IRIG-Pheliqs, 38054 Grenoble, France*

(Received 19 February 2020; revised 22 September 2020; accepted 5 October 2020; published 23 November 2020)

Simulating the Sycamore quantum supremacy circuits

Feng Pan[1,2] and Pan Zhang[1,*]

[1]*Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100190, China*
[2]*School of Physical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China*

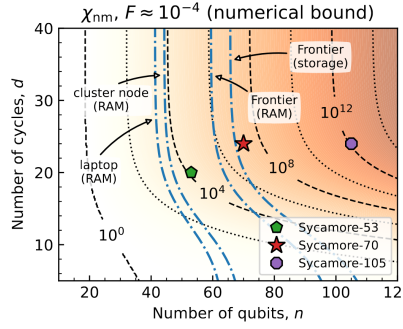
We propose a general tensor network method for simulating quantum circuits. The method is massively more efficient in computing a large number of correlated bitstring amplitudes and probabilities than existing methods. As an application, we study the sampling problem of Google's Sycamore circuits, which are believed to be beyond the reach of classical supercomputers and have been used to demonstrate quantum supremacy. Using our method, employing a small computational cluster containing 60 graphical processing units (GPUs), we have generated one million correlated bitstrings with some entries fixed, from the Sycamore circuit with 53 qubits and 20 cycles, with *linear cross-entropy benchmark* (XEB) fidelity equals 0.739, which is much higher than those in Google's quantum supremacy experiments.

Mais en 2024 : la suprématie quantique est stabilisée

Phase Transitions in Random Circuit Sampling

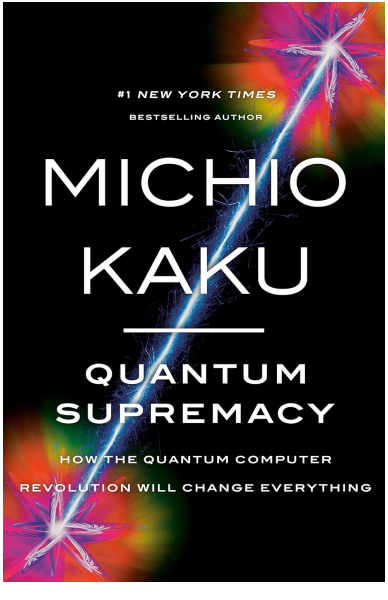
Google Quantum AI and Collaborators

Undesired coupling to the surrounding environment destroys long-range correlations on quantum processors and hinders the coherent evolution in the nominally available computational space. This incoherent noise is an outstanding challenge to fully leverage the computation power of near-term quantum processors [1]. It has been shown that benchmarking Random Circuit Sampling (RCS) with Cross-Entropy Benchmarking (XEB) can provide a reliable estimate of the effective size of the Hilbert space coherently available [2–8]. The extent to which the presence of noise can trivialize the outputs of a given quantum algorithm, i.e. making it spoofable by a classical computation, is an unanswered question. Here, by implementing an RCS algorithm we demonstrate experimentally that there are two phase transitions observable with XEB, which we explain theoretically with a statistical model. The first is a dynamical transition as a function of the number of cycles and is the continuation of the anti-concentration point in the noiseless case. The second is a quantum phase transition controlled by the error per cycle; to identify it analytically and experimentally, we create a weak link model which allows varying the strength of noise versus coherent evolution. Furthermore, by presenting an RCS experiment with 67 qubits at 32 cycles, we demonstrate that the computational cost of our experiment is beyond the capabilities of existing classical supercomputers, even when accounting for the inevitable presence of noise. Our experimental and theoretical work establishes the existence of transitions to a stable computationally complex phase that is reachable with current quantum processors.



Exp.	1 amp.	1 million noisy samples		
	FLOPs	FLOPs	XEB fid.	Time
SYC-53 [4]	6×10^{17}	2×10^{17}	2×10^{-3}	6 s
ZCZ-56 [5]	6×10^{19}	6×10^{19}	6×10^{-4}	20 min
ZCZ-60 [6]	1×10^{21}	1×10^{23}	3×10^{-4}	40 days
SYC-70	5×10^{23}	6×10^{25}	2×10^{-3}	50 yr
SYC-67	2×10^{23}	2×10^{37} 2×10^{28} 2×10^{25}	1×10^{-3}	1×10^{13} yr 1×10^{4} yr* 12 yr**

La « hype »



L'ordinateur quantique permettrait :

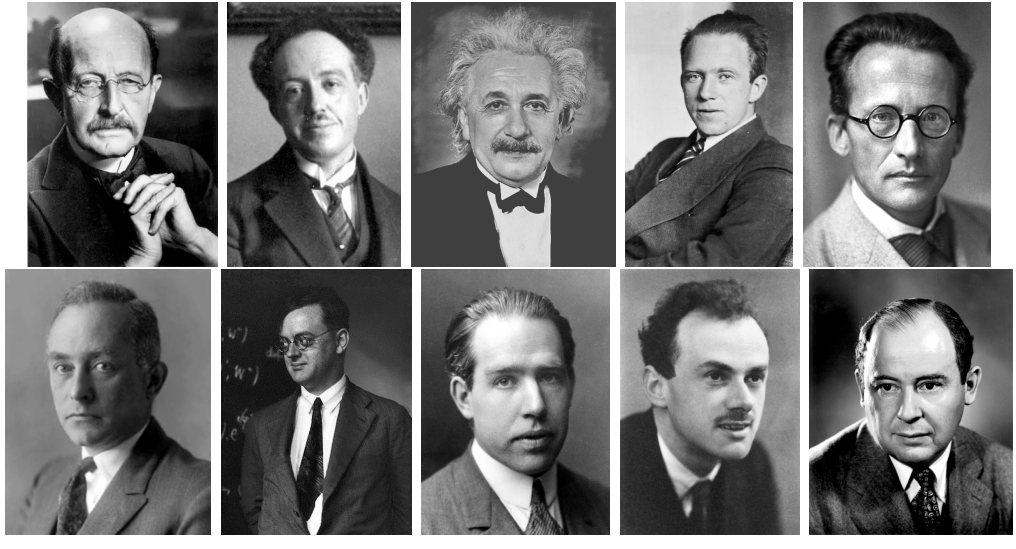
- De résoudre le réchauffement climatique
- De rendre possible l'intelligence artificielle générale

La mécanique quantique

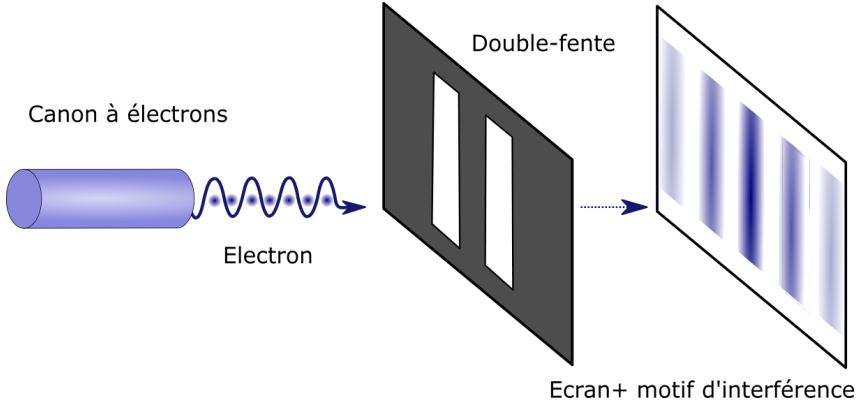
La mécanique contre-intuitive qui régit la dynamique des constituants élémentaires de la matière

Mécanique quantique

Construite progressivement entre 1900 et 1930



Les lois changent dans le monde microscopique



Les lois changent dans le monde microscopique

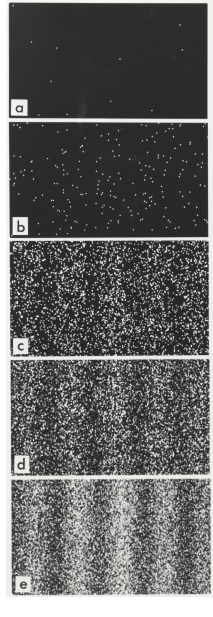
On lance les électrons **un par un** :

- Les impacts sur l'écran sont ponctuels

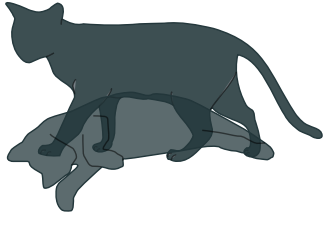
Les lois changent dans le monde microscopique

On lance les électrons **un par un** :

- Les impacts sur l'écran sont ponctuels
- Les impacts se répartissent statistiquement comme une onde !



La nature du réel



Chat de Schrödinger - superposition quantiques

Superpositions quantiques

Tout se passe comme si les particules pouvaient être en même temps dans des positions différentes.

La décohérence

Inobservabilité des superpositions macroscopiques

Les superpositions, *qu'elles soient réelles ou pas*, sont inobservables à notre échelle macroscopique.

Théologie négative de la mécanique quantique

La mécanique quantique a des conséquences surprenantes, mais elle **ne dit pas** :

1. On peut communiquer à distance plus vite que la lumière.

Théologie négative de la mécanique quantique

La mécanique quantique a des conséquences surprenantes, mais elle **ne dit pas** :

1. On peut communiquer à distance plus vite que la lumière.
2. Le réel n'existe pas ou est totalement subjectif.

Théologie négative de la mécanique quantique

La mécanique quantique a des conséquences surprenantes, mais elle **ne dit pas** :

1. On peut communiquer à distance plus vite que la lumière.
2. Le réel n'existe pas ou est totalement subjectif.
3. On peut être *en même temps* des choses incompatibles

Théologie négative de la mécanique quantique

La mécanique quantique a des conséquences surprenantes, mais elle **ne dit pas** :

1. On peut communiquer à distance plus vite que la lumière.
2. Le réel n'existe pas ou est totalement subjectif.
3. On peut être *en même temps* des choses incompatibles

Applications de la première révolution quantique

Sur notre capacité à prédire

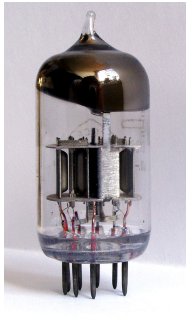
$$a_e = 0.001159652181643(764) \quad \text{théorie}$$
$$a_e = 0.00115965218059(13) \quad \text{expérience}$$

Applications de la première révolution quantique

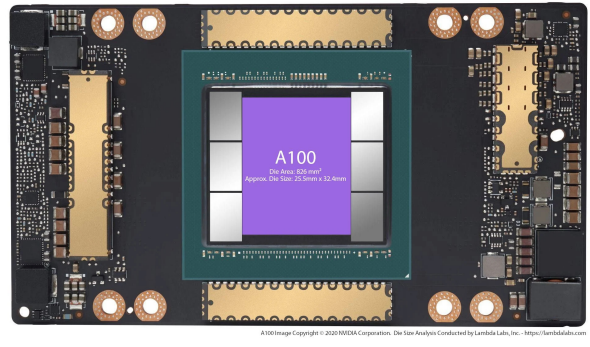
Sur notre capacité à prédire

$$a_e = 0.001159652181643(764) \quad \text{théorie}$$
$$a_e = 0.00115965218059(13) \quad \text{expérience}$$

Sur notre capacité à inventer



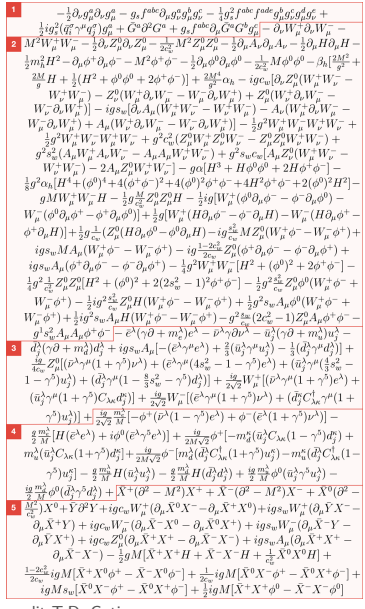
$\longrightarrow$



Théorie quantique des champs

Mécanique quantique + relativité restreinte = Théorie quantique des champs

Théorie des champs particulière incluant les 3 forces = Modèle Standard



credit T.D. Gutierrez

Le problème à N corps quantique

L'épine dans le pied du réductionnisme

Le problème à N corps quantique

Équation de Schrödinger

$$i\hbar\frac{\partial\psi}{\partial t} = H\psi$$

La fonction d'onde ψ contient D^N variables (ou paramètres libres) où

- $D \geqslant 2$ est le nombre d'états accessible à une particule
- N est le nombre de particules

Le problème à N corps quantique

Équation de Schrödinger a D^N variables

Le plus simple : $D = 2$ états possibles

Le problème à N corps quantique

Équation de Schrödinger a D^N variables

Le plus simple : $D = 2$ états possibles

- cube $3 \times 3 \times 3 = 27$ particules – équation de Schrödinger résoluble sur cet ordinateur

Le problème à N corps quantique

Équation de Schrödinger a D^N variables

Le plus simple : $D = 2$ états possibles

- cube $3 \times 3 \times 3 = 27$ particules – équation de Schrödinger résoluble sur cet ordinateur
- cube $4 \times 4 \times 4 = 64$ particules – insoluble même avec Frontier

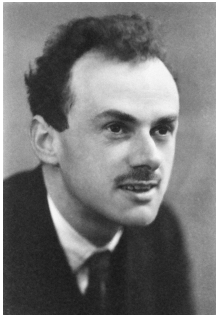
Le problème à N corps quantique

Équation de Schrödinger a D^N variables

Le plus simple : $D = 2$ états possibles

- cube $3 \times 3 \times 3 = 27$ particules – équation de Schrödinger résoluble sur cet ordinateur
- cube $4 \times 4 \times 4 = 64$ particules – insoluble même avec Frontier
- cube $5 \times 5 \times 5$ pas assez de silicium sur Terre...

Compris par Paul Dirac dès 1930



Quantum Mechanics of Many-Electron Systems.

By P. A. M. Dirac, St. John's College, Cambridge.

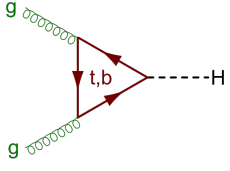
(Communicated by R. H. Fowler, F.R.S.—Received March 12, 1929.)

§ 1. *Introduction.*

The general theory of quantum mechanics is now almost complete, the imperfections that still remain being in connection with the exact fitting in of the theory with relativity ideas. These give rise to difficulties only when high-speed particles are involved, and are therefore of no importance in the consideration of atomic and molecular structure and ordinary chemical reactions, in which it is, indeed, usually sufficiently accurate if one neglects relativity variation of mass with velocity and assumes only Coulomb forces between the various electrons and atomic nuclei. The underlying physical laws necessary for the mathematical theory of a large part of physics and the whole of chemistry are thus completely known, and the difficulty is only that the exact application of these laws leads to equations much too complicated to be soluble. It therefore becomes desirable that approximate practical methods of applying quantum mechanics should be developed, which can lead to an explanation of the main features of complex atomic systems without too much computation.

Problèmes ouverts de physique théorique

Physique fondamentale

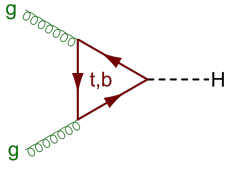


Interaction forte entre quarks et gluons

Permet la formation du noyaux

Problèmes ouverts de physique théorique

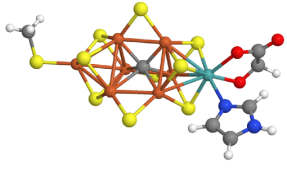
Physique fondamentale



Interaction forte entre quarks et gluons

Permet la formation du noyaux

Chimie

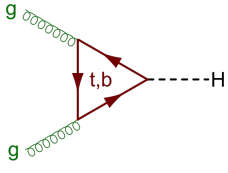


Interactions électrons-électrons et électron-protons

Permet la formation de molécules complexes

Problèmes ouverts de physique théorique

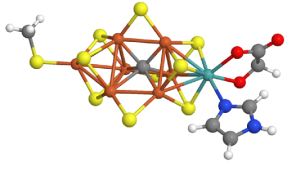
Physique fondamentale



Interaction forte entre quarks et gluons

Permet la formation du noyaux

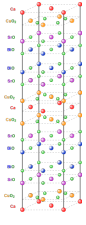
Chimie



Interactions électrons-électrons et électron-protons

Permet la formation de molécules complexes

Condensed matter

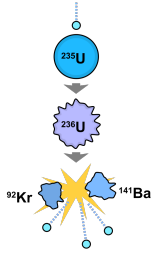


Interaction forte entre électrons

Permet la supraconductivité des cuprates

Conséquences pratiques

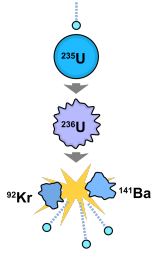
Physique nucléaire



Les propriétés du noyau sont mesurées

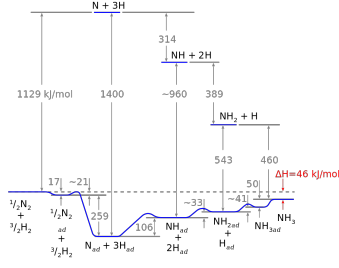
Conséquences pratiques

Physique nucléaire



Les propriétés du noyau sont mesurées

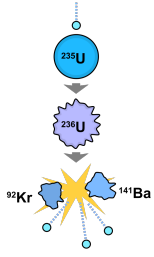
Catalyse



L'amoniac est energivore $\geqslant 1\%$ CO2 mondial

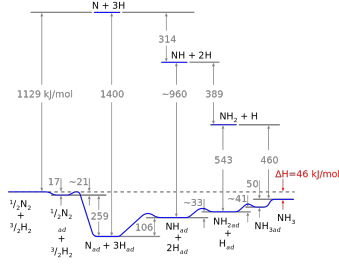
Conséquences pratiques

Physique nucléaire



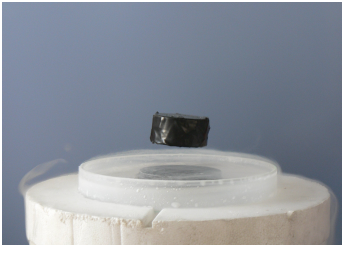
Les propriétés du noyau sont mesurées

Catalyse



L'amoniac est energivore $\geqslant 1\%$ CO2 mondial

Supraconducteurs haute T_c



Pas de transfert d'électricité sans perte

L'ordinateur quantique

Le renversement du problème à N corps

L'intuition de Richard Feynman

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

« La nature n'est pas classique, bon sang, et si vous voulez faire une simulation de la nature, vous feriez mieux rendre la simulation quantique, et parbleu c'est un problème merveilleux, parce que cela ne semble pas si facile. »

Du simulateur quantique à l'ordinateur quantique

Idem : l'idée de Feynman d'un simulateur quantique analogique a été améliorée en ordinateur quantique digital.

1. Résultats arbitrairement précis
2. Erreurs corrigeables

Une application non quantique : RSA

Question de multiplication

Que vaut

64 135 289 477 071 580 278 790 190 170 577 389 084 825 014 742 943 447 208 116 859 632 024 532 344 630 238 623 598 752 668 347 708 737 661 925 585 694 639 798 853 367

$\times$

33 372 027 594 978 156 556 226 010 605 355 114 227 940 760 344 767 554 666 784 520 987 023 841 729 210 037 080 257 448 673 296 881 877 565 718 986 258 036 932 062 711

?

Réponse

2 140 324 650 240 744 961 264 423 072 839 333 563 008 614 715 144 755 017
797 754 920 881 418 023 447 140 136 643 345 519 095 804 679 610 992 851
872 470 914 587 687 396 261 921 557 363 047 454 770 520 805 119 056 493
106 687 691 590 019 759 405 693 457 452 230 589 325 976 697 471 681 738
069 364 894 699 871 578 494 975 937 497 937

Question de factorisation

Trouver les nombres premiers p et q tels que

$p \times q =$

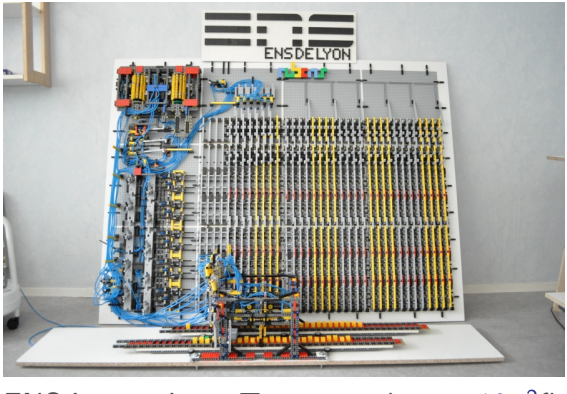
2 140 324 650 240 744 961 264 423 072 839 333 563 008 614 715 144 755 017
797 754 920 881 418 023 447 140 136 643 345 519 095 804 679 610 992 851
872 470 914 587 687 396 261 921 557 363 047 454 770 520 805 119 056 493
106 687 691 590 019 759 405 693 457 452 230 589 325 976 697 471 681 738
069 364 894 699 871 578 494 975 937 497 937

Trouver les nombres premiers p et q tels que

$p \times q =$

2 519 590 847 565 789 349 402 718 324 004 839 857 142 928 212 620 403 202
777 713 783 604 366 202 070 759 555 626 401 852 588 078 440 691 829 064
124 951 508 218 929 855 914 917 618 450 280 848 912 007 284 499 268 739
280 728 777 673 597 141 834 727 026 189 637 501 497 182 469 116 507 761
337 985 909 570 009 733 045 974 880 842 840 179 742 910 064 245 869 181
719 511 874 612 151 517 265 463 228 221 686 998 754 918 242 243 363 725
908 514 186 546 204 357 679 842 338 718 477 444 792 073 993 423 658 482
382 428 119 816 381 501 067 481 045 166 037 730 605 620 161 967 625 613
384 414 360 383 390 441 492 634 432 190 114 657 544 454 178 424 020 924
616 515 723 350 778 707 749 817 125 772 467 962 926 386 356 373 289 912
154 831 438 167 899 885 040 445 364 023 527 381 951 378 636 564 391 212
010 397 122 822 120 720 357

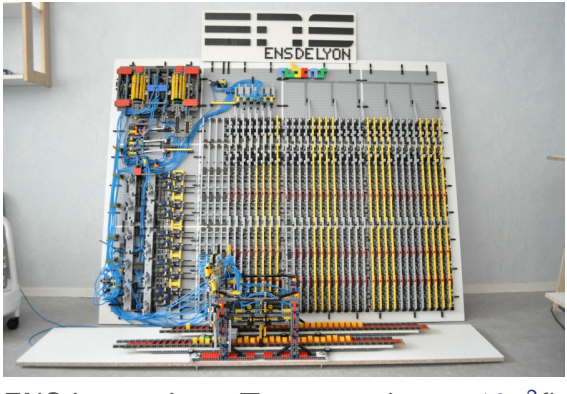
Factoriser sur un ordinateur « classique »



ENS Lyon – Lego Turing machine $\sim 10^{-2}$flops

Oak ridge – Summit $\sim 10^{17}$ flops

Factoriser sur un ordinateur « classique »



ENS Lyon – Lego Turing machine $\sim 10^{-2}$flops

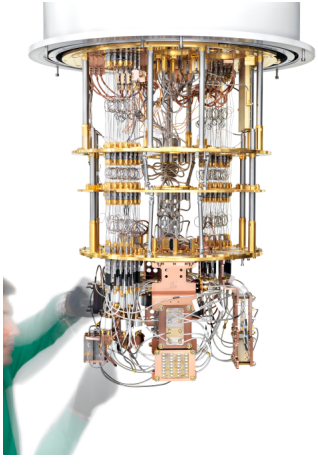
Oak ridge – Summit $\sim 10^{17}$ flops

Trouver p et q pour un nombre à N chiffres prend un temps

$$t_{\text{Lego}} = C_{\text{Lego}} \ \exp(\sqrt[3]{N})$$

$$t_{\text{Summit}} = C_{\text{Summit}} \ \exp(\sqrt[3]{N})$$

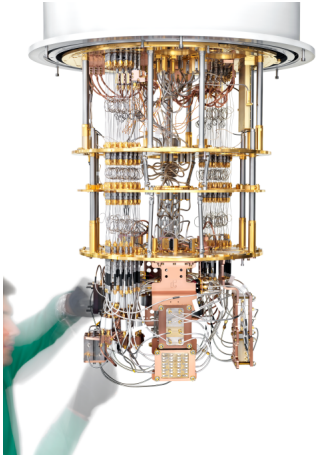
Factoriser sur un ordinateur quantique



- Tout ordinateur classique

$$t = C \exp\left(\sqrt[3]{N}\right)$$

Factoriser sur un ordinateur quantique



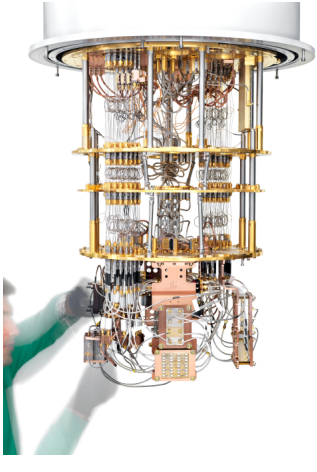
- Tout ordinateur classique

$$t = C \exp\left(\sqrt[3]{N}\right)$$

- Algorithme de Shor sur un ordinateur quantique

$$t = C_q \, N^3$$

Factoriser sur un ordinateur quantique



- Tout ordinateur classique

$$t = C \exp\left(\sqrt[3]{N}\right)$$

- Algorithme de Shor sur un ordinateur quantique

$$t = C_q \, N^3$$

L'ordinateur quantique est plus lent $C_q \gg C_{\text{Summit}}$ mais ne sent pas la difficulté augmenter !

Conséquence pratique

L'algorithme RSA n'est pas sûr

Un ordinateur quantique pourra casser RSA-2048 en quelques heures. Augmenter la taille des clés n'aidera pas.

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ?

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ? $\rightarrow$ pas sûr

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ? $\rightarrow$ pas sûr
- Intelligence artificielle ?

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ? $\rightarrow$ pas sûr
- Intelligence artificielle ? $\rightarrow$ probablement pas

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ? $\rightarrow$ pas sûr
- Intelligence artificielle ? $\rightarrow$ probablement pas
- Problèmes liés au réchauffement climatique ?

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ? $\rightarrow$ pas sûr
- Intelligence artificielle ? $\rightarrow$ probablement pas
- Problèmes liés au réchauffement climatique ?$\rightarrow$ peut-être très indirectement

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ? $\rightarrow$ pas sûr
- Intelligence artificielle ? $\rightarrow$ probablement pas
- Problèmes liés au réchauffement climatique ?$\rightarrow$ peut-être très indirectement
- Tester tout en parallèle ?

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ? $\rightarrow$ pas sûr
- Intelligence artificielle ? $\rightarrow$ probablement pas
- Problèmes liés au réchauffement climatique ?$\rightarrow$ peut-être très indirectement
- Tester tout en parallèle ? $\rightarrow$ **non**

Autres applications ?

Hors du problème à N corps et de la factorisation rapide

- Optimisation ? $\rightarrow$ pas sûr
- Intelligence artificielle ? $\rightarrow$ probablement pas
- Problèmes liés au réchauffement climatique ?$\rightarrow$ peut-être très indirectement
- Tester tout en parallèle ? $\rightarrow$ **non**

Pour le moment : le problème à N corps est l'application la plus utile !

Comment fabriquer un ordinateur quantique ?

La bataille contre la décohérence

Du transistor au qubit

$\longrightarrow$? ? ? ? ?

Qubit

Particule ou objet quantique qui peut encoder de l'information en préservant les superpositions quantiques

Candidats

Explorés par les laboratoires académiques et l'industrie :

- Atomes individuels piégés par laser [Quera, Pasqal, Planqc]
- Ions individuel piégés par laser [IonQ, Quantinuum]
- Spins dans du silicium [QuTech, CEA]
- Photons [PsiQuantum,]
- Courants supraconducteurs [IBM, Google, Amazon, Alice & Bob]
- ...

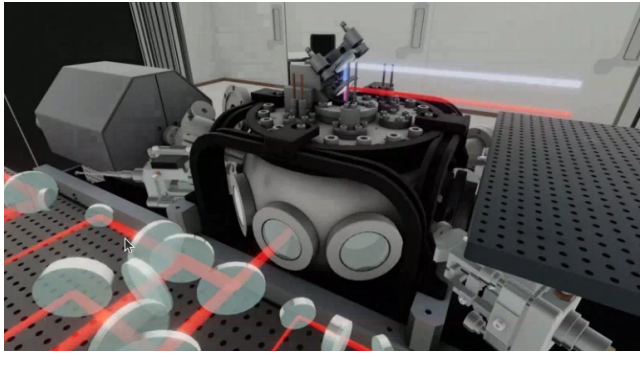
La bataille contre la décohérence

Deux solutions contre la décohérence

- Mieux protéger le qubit de son environnement
- Utiliser plusieurs qubits physiques pour un qubit logique

Pasqal

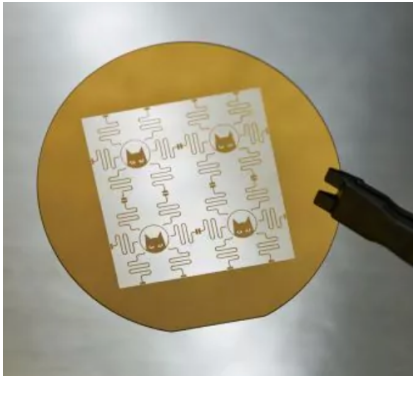
Startup issue de la recherche de l'institut d'Optique

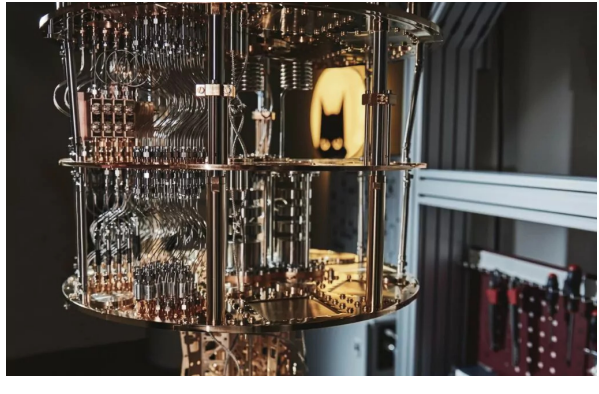


Stratégie similaire à celle de Quera / Harvard (mais démarrage antérieur)

Alice et Bob

Startup issue de la recherche École Normale Supérieure / Mines / Inria



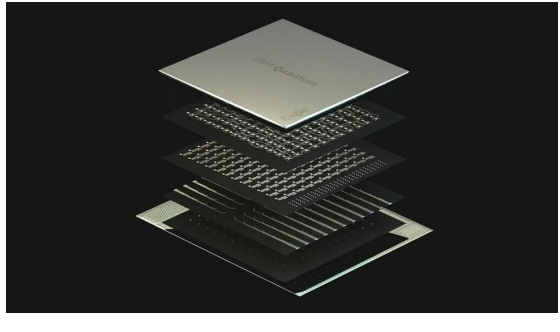


Stratégie similaire à celle d'Amazon (mais démarrage antérieur !)

Vers la suprématie utile ?

IBM – 14 juin 2023 dans *Nature*

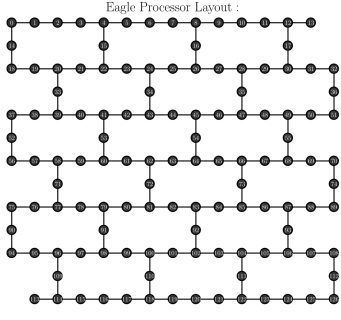
Evidence for the utility of quantum computing before fault tolerance

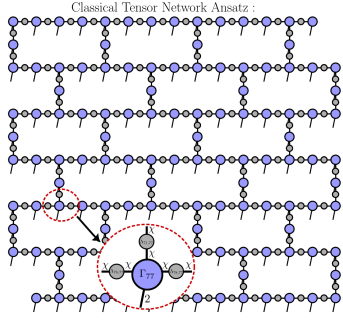


- 127 qubits à base de boucles supraconductrices
- premier exemple de suprématie utile ?

Pas encore

Flatiron – 26 juin 2023 sur `ArXiv`
Efficient tensor network simulation of IBM's Eagle [...]





- Simulation du même problème avec un ordinateur classique
- Meilleure précision que l'ordinateur quantique !

Conclusion

- On connaît quasi exactement les lois de la nature (mécanique quantique + relativité restreinte)
- Ces lois quantiques sont difficiles à simuler [Dirac]
- On peut utiliser la nature elle même pour la simulation [Feynman]
- Cette puissance quantique est utilisable pour factoriser de gros nombres
- Il existe probablement d'autres applications mais rien d'évident
- L'ordinateur quantique sera plus lent pour la quasi totalité des tâches
- Les proto ordinateurs quantiques qui existent ne sont pas encore utiles
- L'utilité sur le problème à N corps est proche (quelques années)
- L'utilité sur d'autres applications comme RSA est lointaine (dizaines d'années)