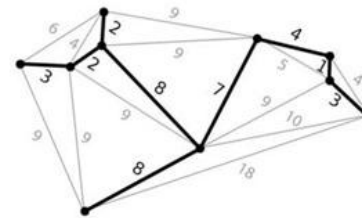
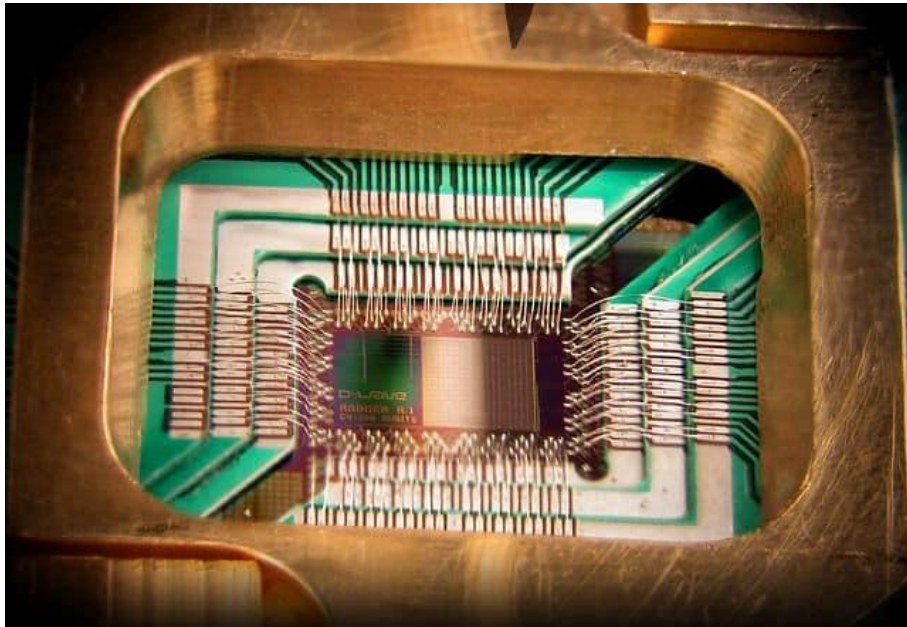


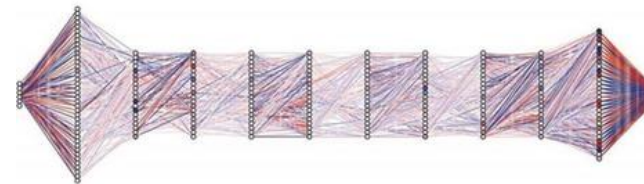
L'ordinateur quantique

Applications et perspectives d'avenir

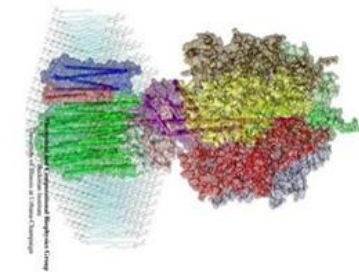




optimisations combinatoires
trajets, placements, cartes



entraînement
de réseaux de neurones



simulations moléculaires
matériaux et biologie

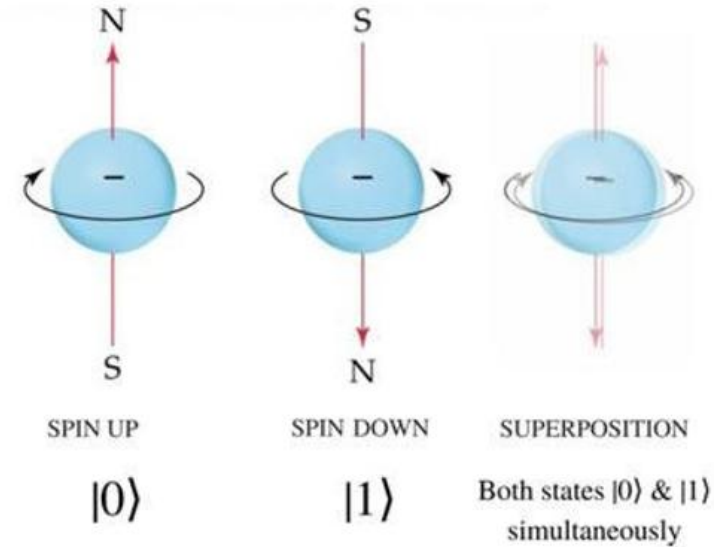
44 988 956 872 684 695 711 909 595 661 757 551 737 391 461 381 495 437 962 032 535 214 %
847 417 212 499 752 572 232 401 732 123 638 539 143 471 977 710 243 318 508 178 915 %
016 041 310 810 028 749 680 395 948 695 236 435 887 854 444 086 897 885 594 538 713 %
228 936 606 776 470 635 385 948 772 950 847 349 789 474 010 570 972 468 331 714 191 %
425 331 349 515 850 718 358 938 779 081 862 288 937 248 229 481 122 957 649 663 638 %
693 717 318 212 628 476 797 261 511 198 103 510 310 449 611 859 242 271 813 366 566 %
997 130 602 961 939 610 490 851 433 975 035 584 182 642 678 405 161 190 698 336 347 %
929 112 811 425 354 268 385 653 335 910 754 799 140 572 752 605 907 751 000 463 584 %
653 690 396 162 388 451 026 377 547 259 579 743 647 906 554 252 830 020 138 218 006 %
943 421 190 175 143 130 541 480 857 851 924 532 107 288 336 106

factorisation
de très grands nombres entiers

- 1) Principe de fonctionnement
- 2) Actualité
 - IBM
 - Google
- 3) Applications
 - Cryptographie
 - IA

Principe de fonctionnement

- Superposition quantique



- Le qubit

bits : 0 **ou** 1

qubits : 0 **et** 1

| | | |
|---------|--------------------------------|---------------------------------|
| états | deux états possibles exclusifs | deux états possibles simultanés |
| lecture | 0 ou 1, déterministe | 0 ou 1, probabiliste |

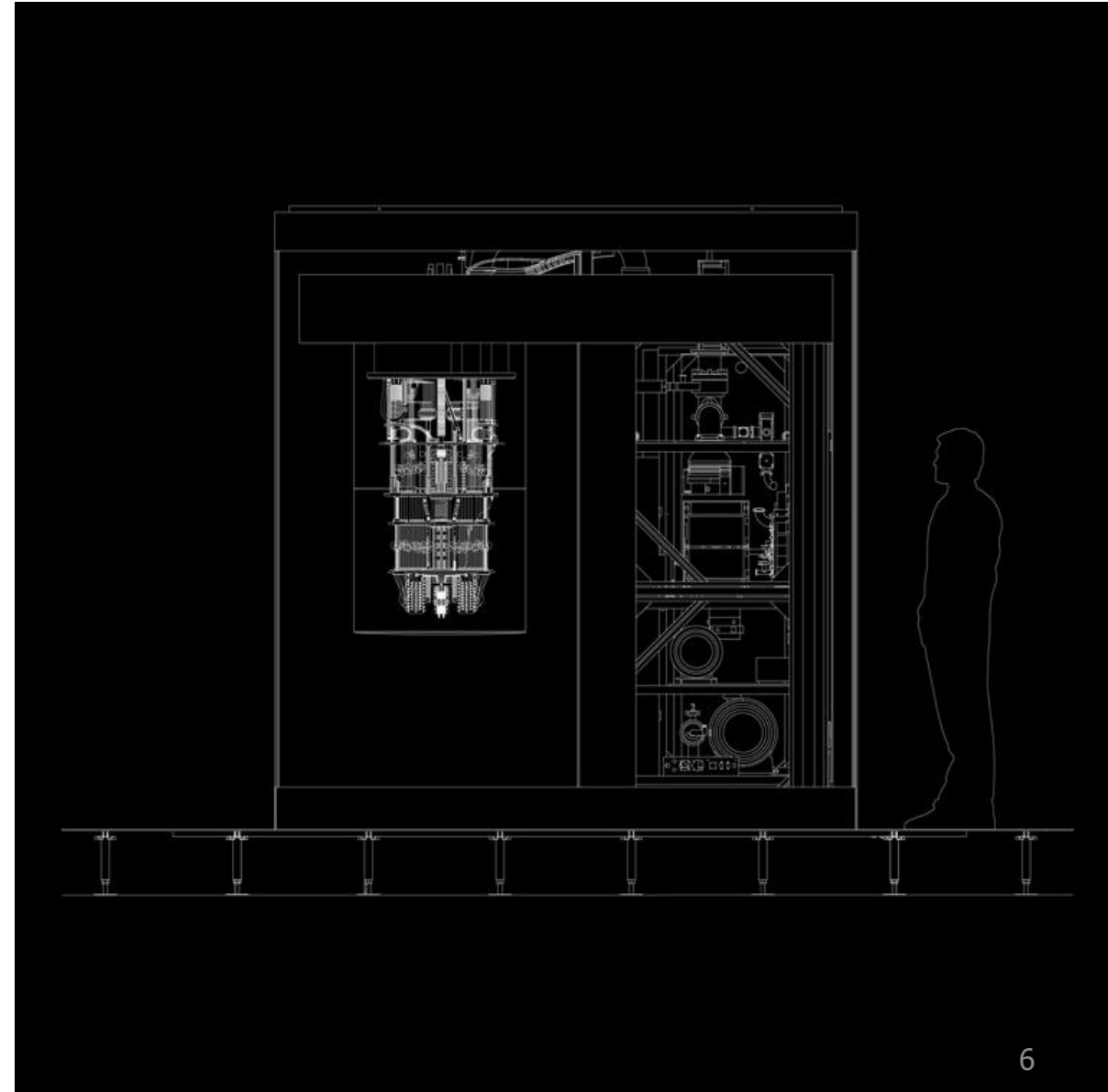
état du qubit $\longrightarrow |\psi\rangle = \alpha |0\rangle + \beta |1\rangle$

probabilité de l'état 0 \downarrow
 probabilité de l'état 1 \downarrow

ACTUALITÉ

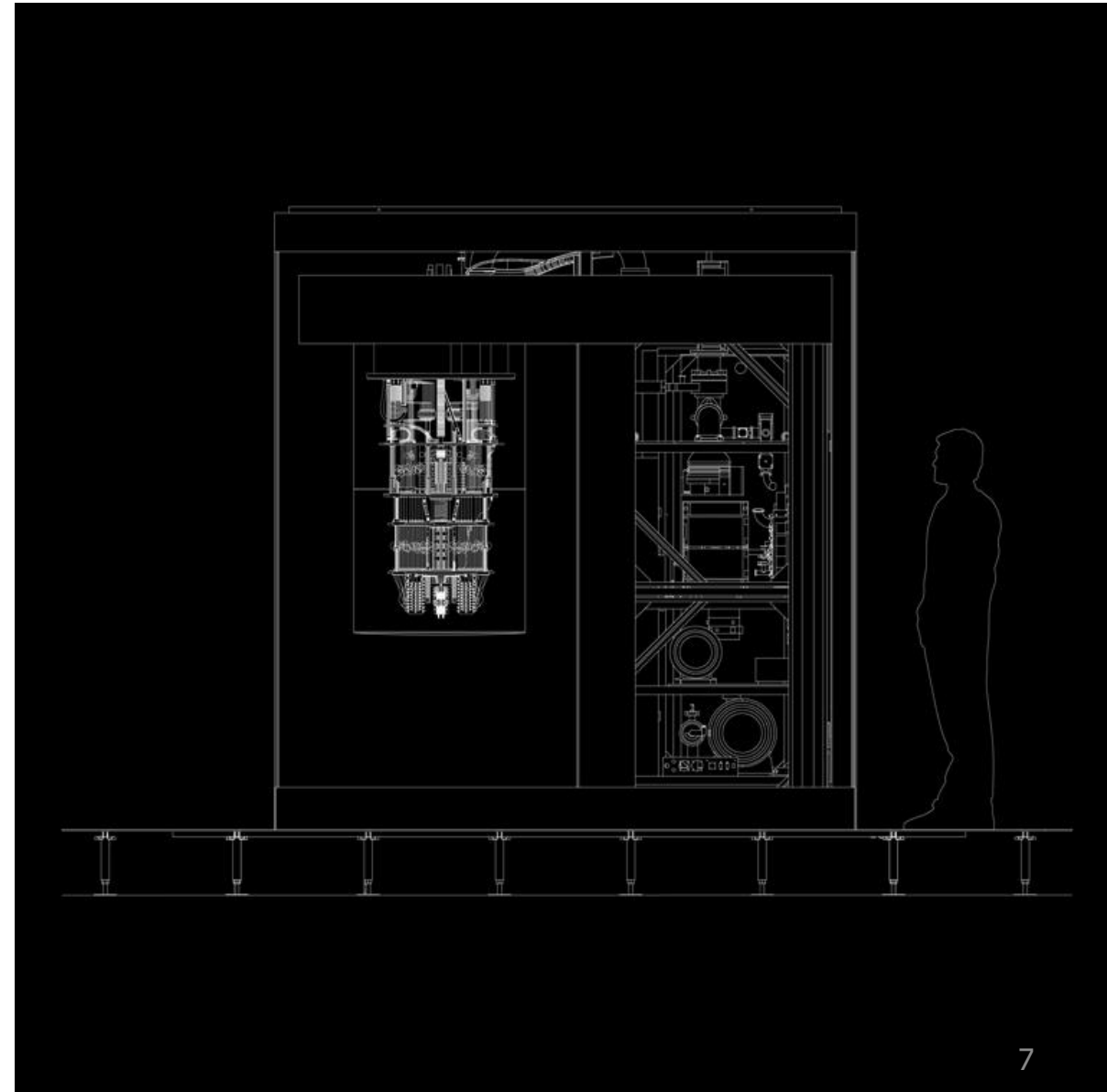
Le nouvel ordinateur quantique d'IBM

- Annoncé au CES 2019
- IBM Q System One
 - 20 qu-bit
 - Accessible sur le cloud
 - Entreprises loue sa capacité de calcul pour un certain temps
 - Possibilité pour les entreprise d'en acheter un
 - Prix pas encore dévoilé




IBM Q System One

- Un système complet et pas seulement un composant séparés
- Modulaire : possibilité de remplacer certaines parties seulement et non le système en entier



Un ordinateur quantique sur le cloud



- IBM proposait déjà les capacités de calculs de leurs ordinateurs quantiques sur le cloud
- Framework Qiskit pour python



Qiskit

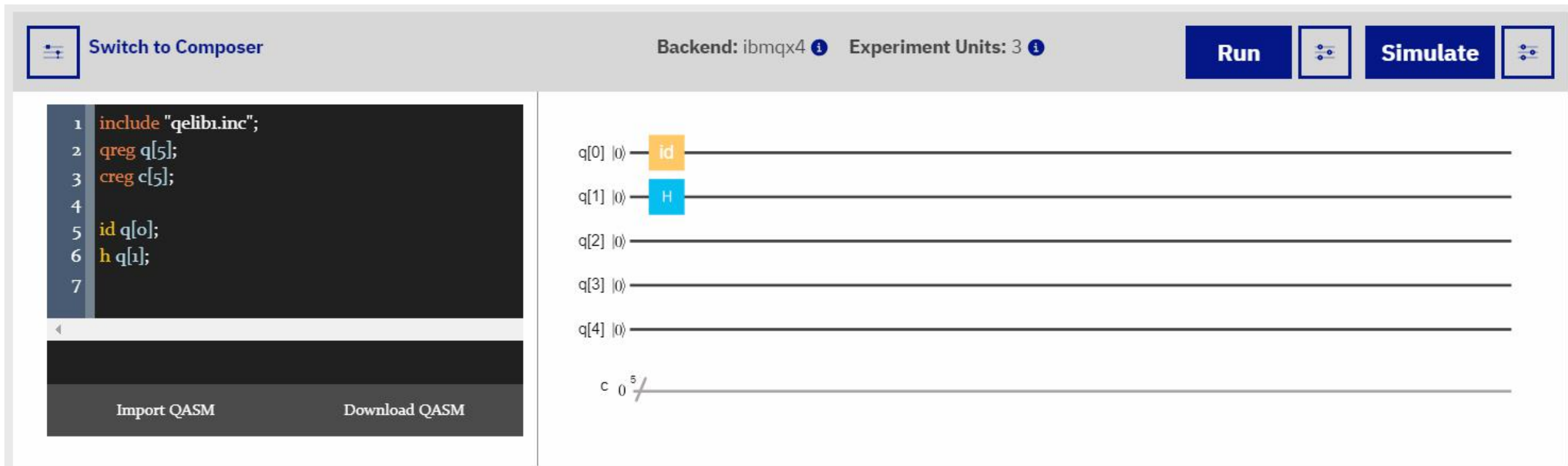
PyPI v0.7.2

An open-source quantum computing framework for leveraging today's quantum processors in research, education, and business

 [GitHub](#)  [Join the Slack community](#)

Un ordinateur quantique sur le cloud

- Interface visuelle







The screenshot displays the Qiskit Composer interface. On the left, a code editor shows the following QASM code:

```
1 include "qelib1.inc";  
2 qreg q[5];  
3 creg c[5];  
4  
5 id q[0];  
6 h q[1];  
7
```

Below the code editor are buttons for "Import QASM" and "Download QASM". The right side of the interface shows a visual representation of the quantum circuit with 5 qubits (q[0] to q[4]) and a classical register (c). The qubits are initialized to $|0\rangle$. The circuit includes an "id" gate on q[0] and an "H" gate on q[1]. The classical register c is shown with a slash and a superscript 5, indicating it is a 5-bit register.

Switch to Composer

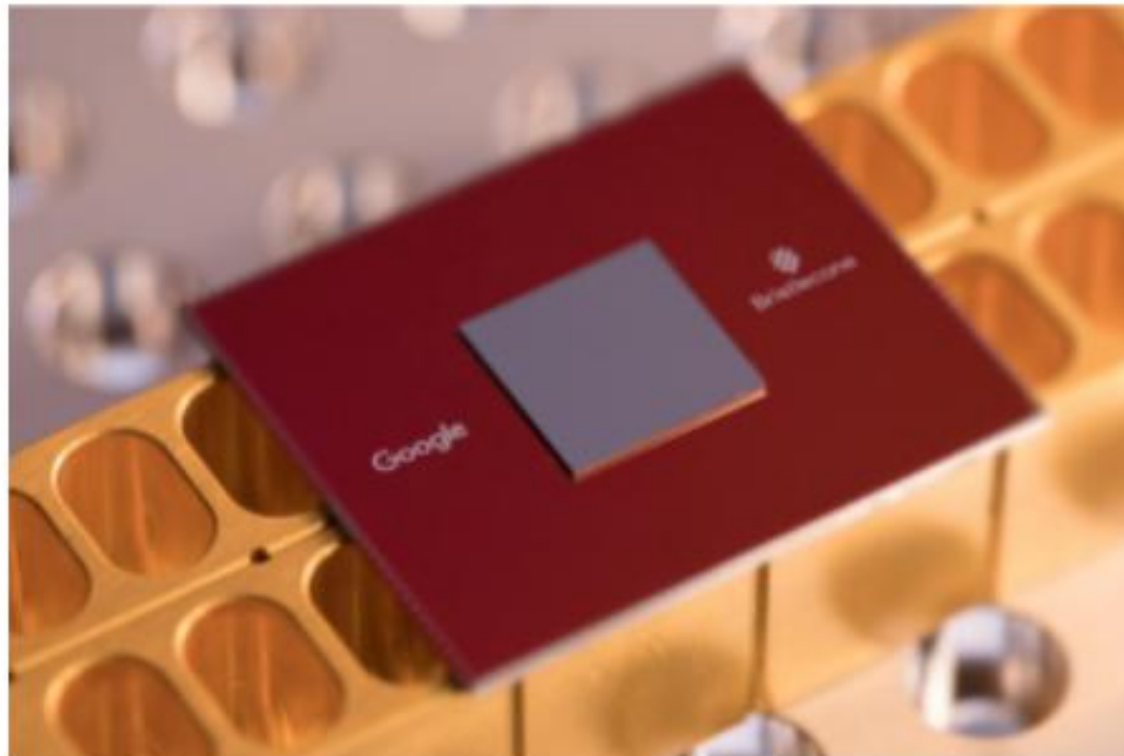
Backend: ibmqx4  Experiment Units: 3 

Run  Simulate 

q[0] $|0\rangle$ — id —
q[1] $|0\rangle$ — H —
q[2] $|0\rangle$ —
q[3] $|0\rangle$ —
q[4] $|0\rangle$ —
c 0⁵ /

Google Bristlecone

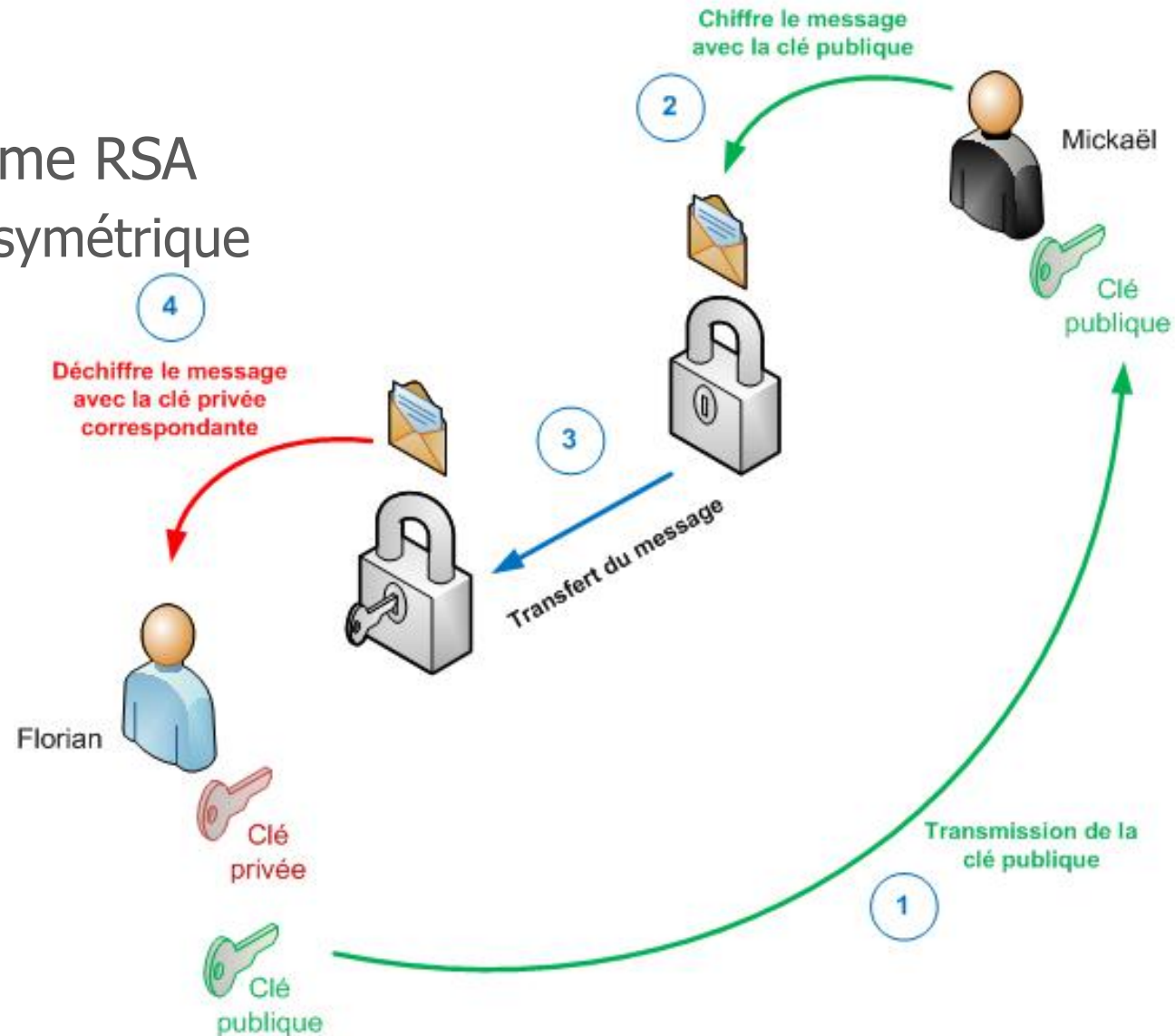
- 72 qubits
- 0.1-1% d'erreur



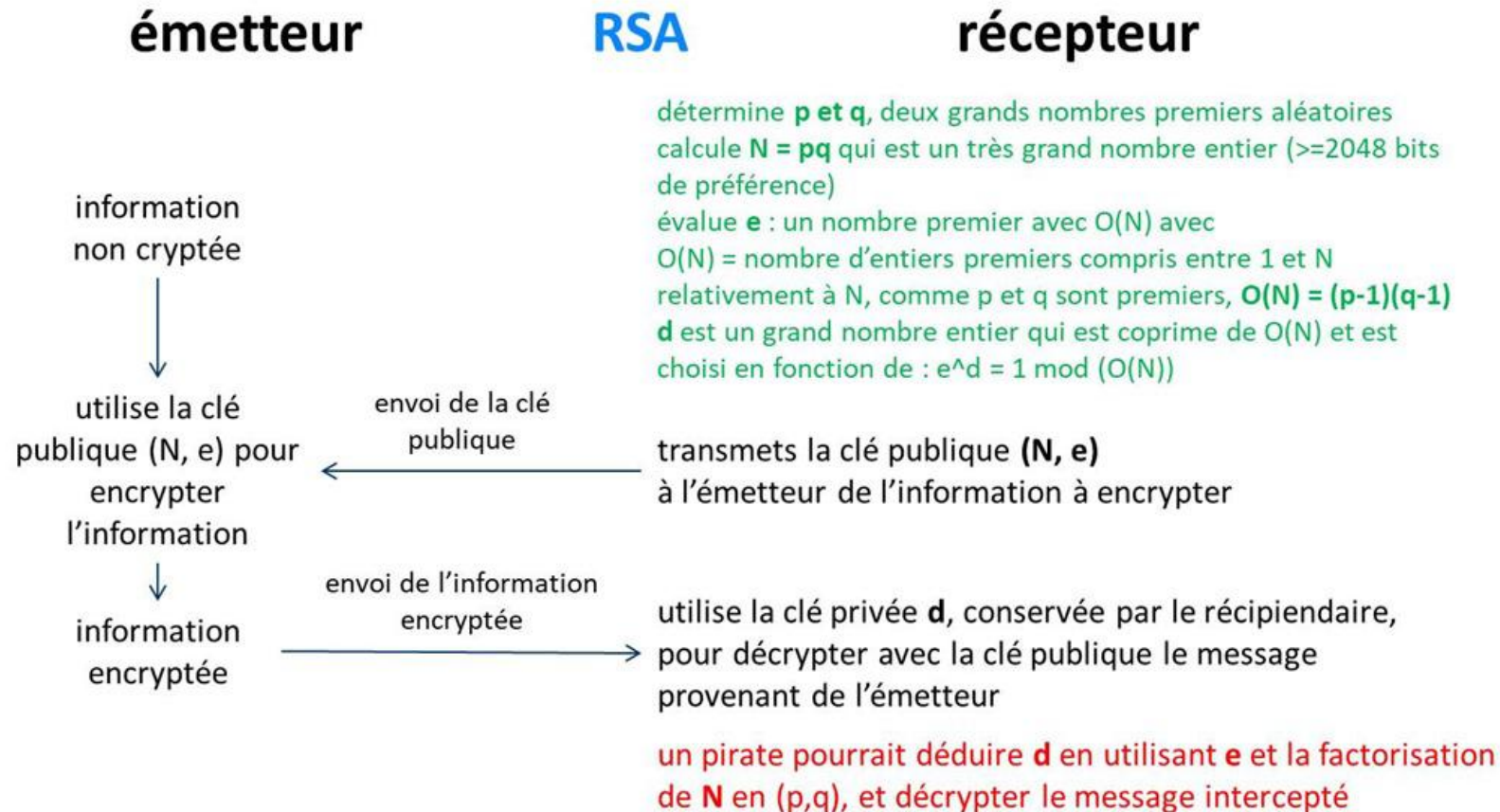


APPLICATIONS

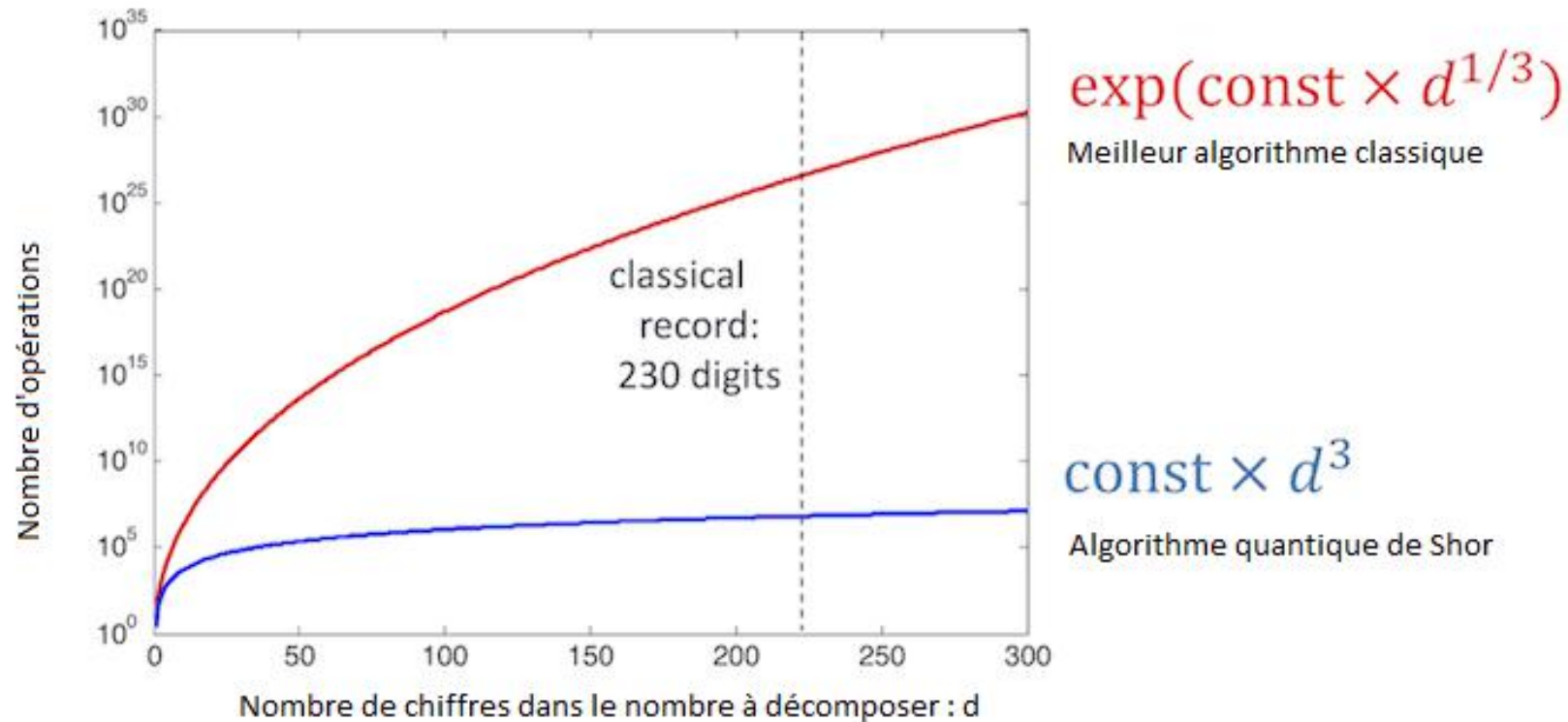
- Principe du système RSA
 - Cryptographie asymétrique



- Principe du système RSA
 - Nombres premiers



- L'algorithme de Shor



- Le Bitcoin
 - utilisation de ECDSA pour les signatures: crackable par ordinateur quantique
 - possibilité de se faire passer pour quelqu'un d'autre dans une transaction

La cryptographie

- Menace éloignée
 - Pas d'ordinateurs assez puissant pour l'instant
- Pour les Bitcoins, des solutions existent
 - Utiliser l'AES en plus

- Capacité de calculs supérieures
- Capacité de traiter une base de donnée plus rapidement
- Combinaison AI et ordinateur quantique pour Big Data
- Google AI Quantum
 - Recherche sur des réseaux de neurones avec superposition d'états
- Utiliser IA pour améliorer l'erreur des ordinateurs quantiques

- Twitter et TweetDeck
 - notamment #quantumcomputer
- Scoop.It!
 - Trouver des articles intéressant
 - Faire mon propre topic
- Diigo
 - Gérer les articles et les sauvegarder pour les lire / y revenir plus tard

délai de mise au point d'OQ universels



Bernard Ourghanlian



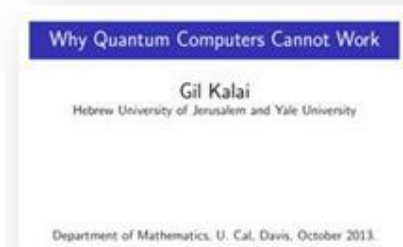
Alain Aspect



Gil Kalai



10000 qubits
99,99% fiables



Et ensuite ?

- Étudier d'autres applications que la cryptographie ou l'IA tel que la médecine
- Étudier les portes quantiques

Merci pour votre attention



ÉCOLE
CENTRALE LYON

36 av. Guy de Collongue
69134 Écully cedex
T + 33 (0)4 72 18 60 00
www.ec-lyon.fr