Certifier la génération de nombres aléatoires avec le quantique

Séminaire au Collège de France, 14 Avril 2021,

Dans le cadre du cours du professeur invité Frédéric Magniez

THOMAS VIDICK

CALIFORNIA INSTITUTE OF TECHNOLOGY

vidick@caltech.edu

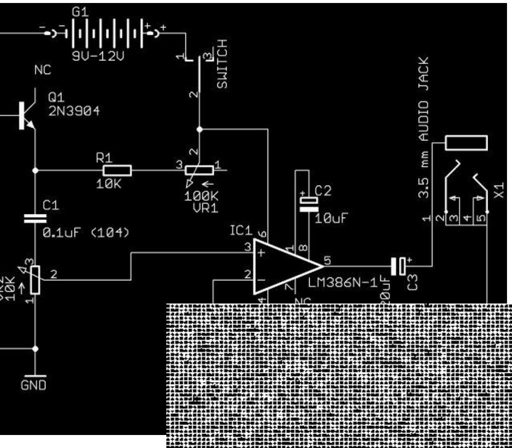
Quantique et aléatoire

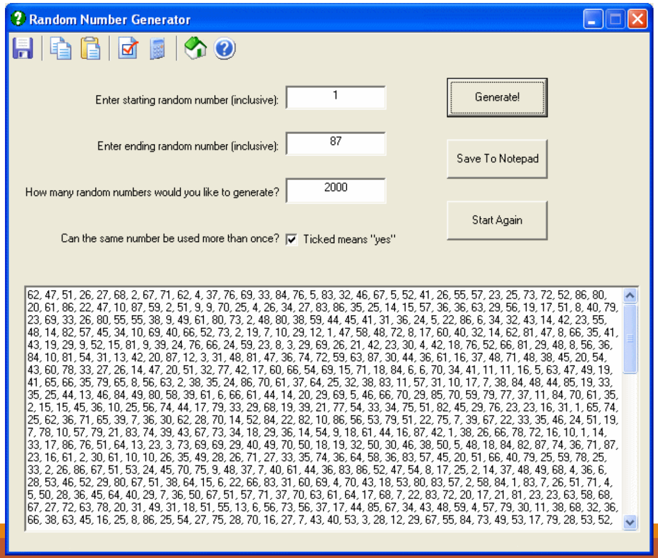
Nombres aléatoires: une ressource fondamentale

- Cryptographie (sans aléas, pas de secrets)
- Algorithmes probabilistes
- Salles de jeux
- Décisions au quotidien

Les ordinateurs classiques sont déterministes

- Génération “pseudo-aléatoire”





Quantique et aléatoire

Nombres aléatoires: une ressource fondamentale

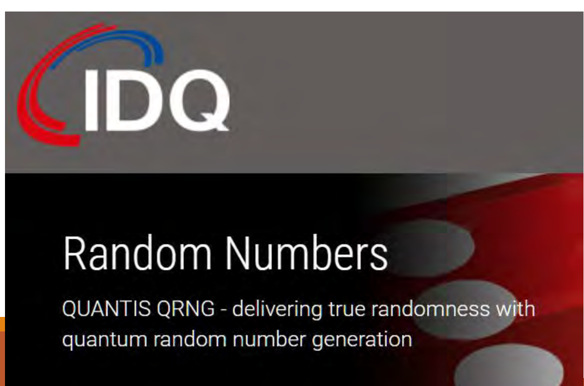
- Cryptographie (sans aléas, pas de secrets)
- Algorithmes probabilistes
- Salles de jeux
- Décisions au quotidien

Les ordinateurs classiques sont déterministes

- Génération “pseudo-aléatoire”

La mécanique quantique est probabiliste

- Génération de nombres “100% aléatoire”?



USB

OEM

PCIe

Quantis Appliance

Le problème de vérification

"There is no such thing as a random number
— there are only methods to produce random numbers"

John von Neumann

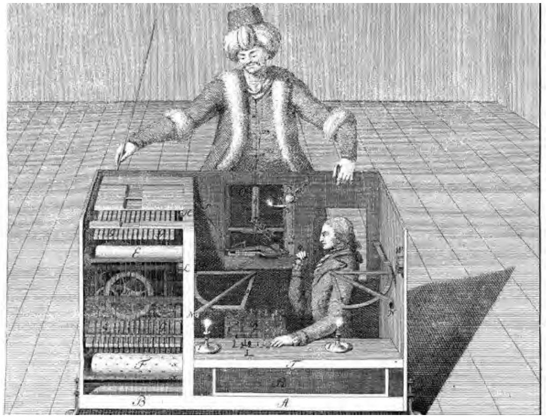
Il n'y a rien de tel qu'un nombre aléatoire
— Il n'y a que des processus de génération de nombres aléatoires

Peut-on *tester* les processus quantiques?

Le problème de vérification

Calcul quantique 1.0

- [Shor’94],[Aharonov-Ben-Or,Gottesman,Shor,Preskill ‘96-97]
  Les ordinateurs quantiques “existent”, peuvent être robustes aux erreurs, et factorisent en temps polynomial

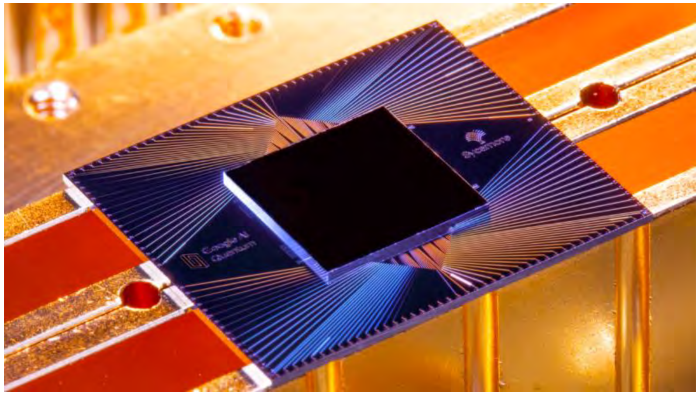


“Mechanical Turk”

[… 20 ans plus tard …]

Calcul quantique 2.0

- [Preskill’18] L’ère “NISQ”
- Toujours pas de tolérance d’erreurs…
  … mais on approche un test de la thèse Church-Turing algorithmique?
- Comment caractériser et vérifier les processus quantiques?



Google “Sycamore,” 53 qubits

Le problème de vérification

Propriétés caractéristiques de l'ordinateur quantique:

1. Complexité exponentielle

   Les algorithmes quantiques exploitent un phénomène d'interférence entre un nombre exponentiel de trajectoires

- Superposition uniforme sur $|x\rangle$, évaluation de f et mesure d'une image y:

$$\frac{1}{\sqrt{2}}|x_0\rangle + \frac{1}{\sqrt{2}}|x_0 \oplus s\rangle$$

- Transformée de Fourier quantique: d tel que $d \cdot s = 0$
- Répéter $O(n)$ fois et déduire s

Le problème de vérification

Propriétés charactéristiques de l’ordinateur quantique:

1. Complexité exponentielle

→ simulation directe impossible

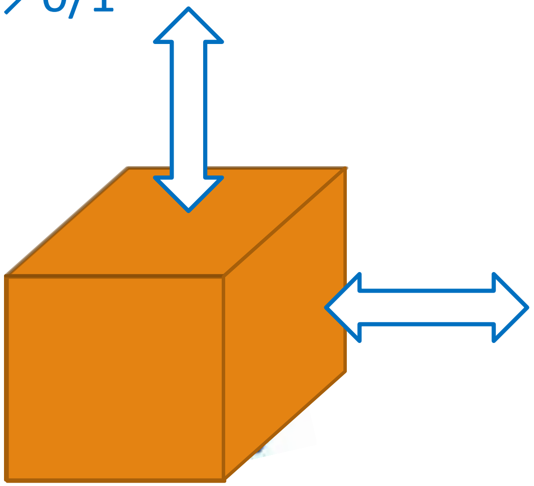
©Intel Tangle Lake (49Q)

2. Mesure-perturbation

Mesure-perturbation

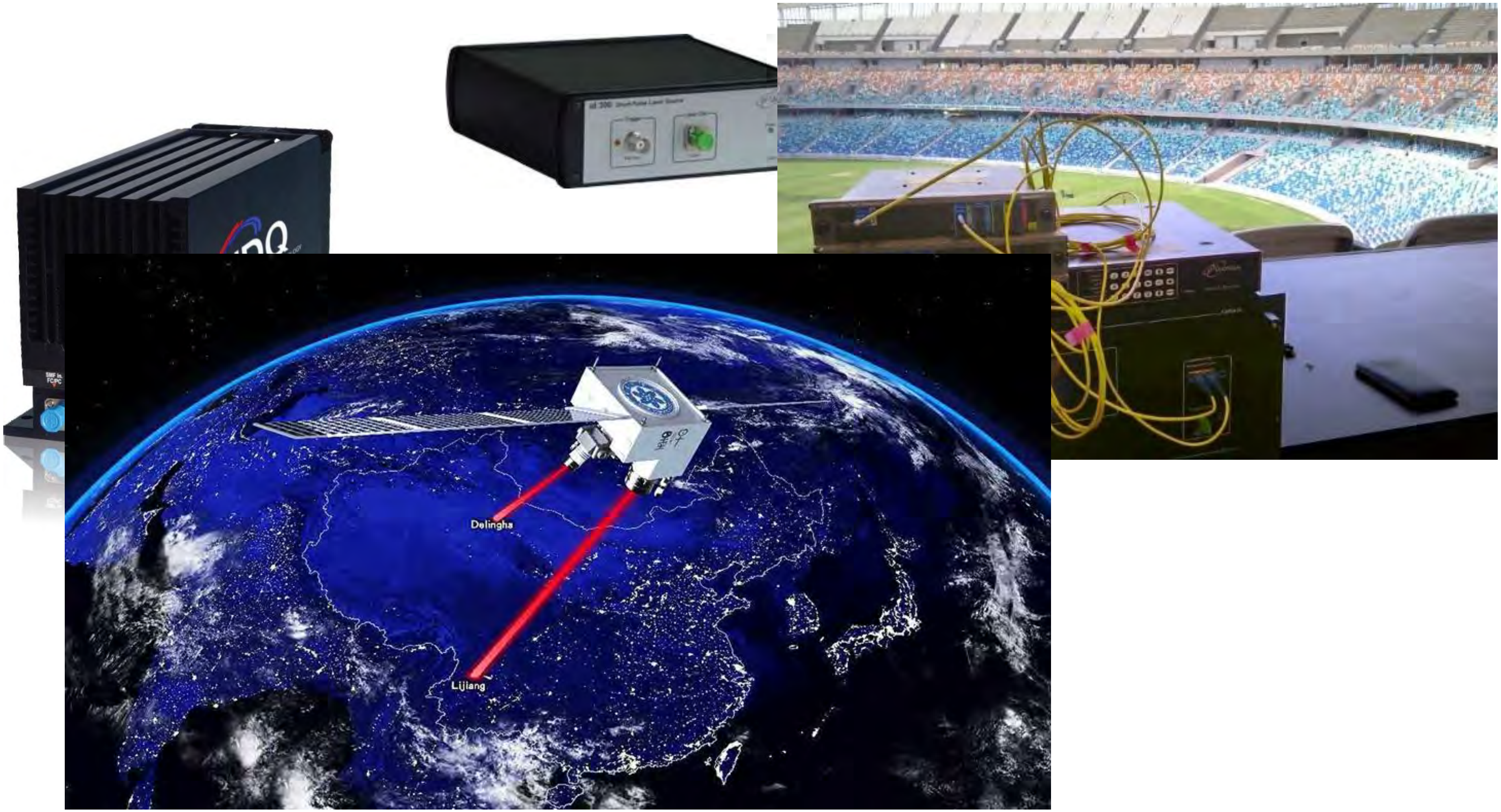
- Wiesner 1968
  <u>Conjugate coding</u>
  SIGACT News 1983

principe d'incertitude ⇒ Possibilités nouvelles pour encoder l'information



Principe d'incertitude: $\Delta Z \; \Delta X \geq h$

Distribution de clé quantique

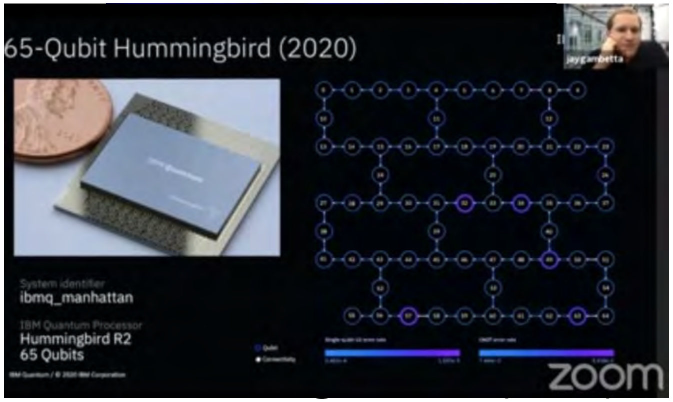


Le problème de vérification

Propriétés characteristiques de l'ordinateur quantique:

1. Complexité exponentielle

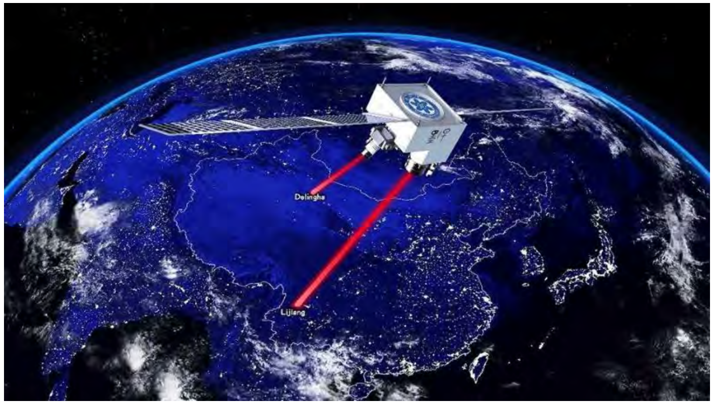
→ simulation directe impossible



2. Mesure-perturbation

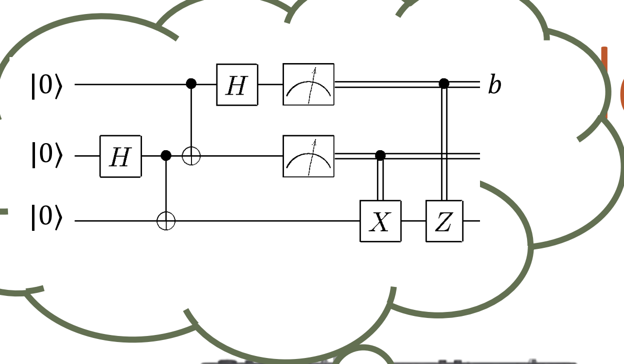
→ le principe d'incertitude

préclut l'observation directe



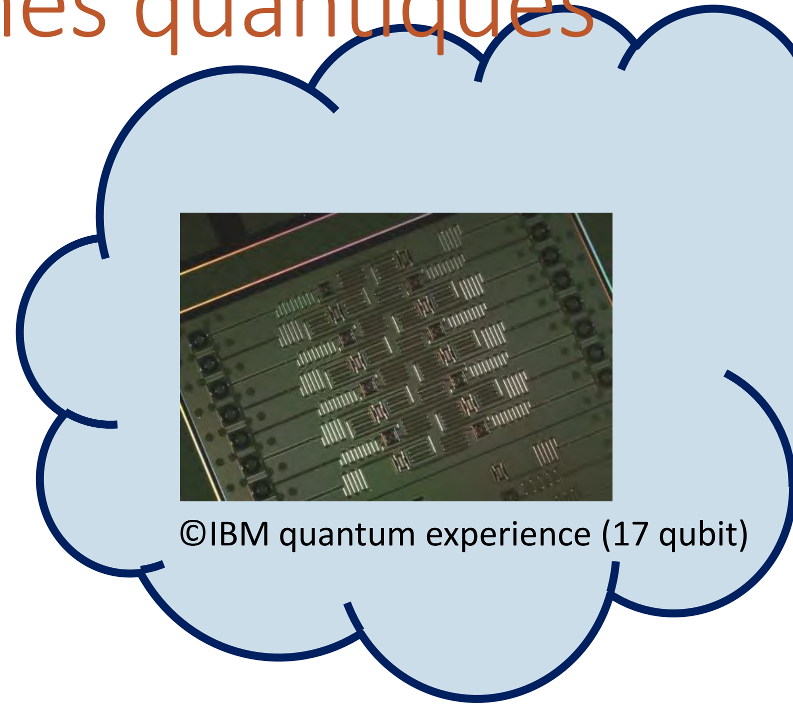
Vérification de processus calculatoires quantiques

le programmes quantiques



communication

classique



©IBM quantum experience (17 qubit)

vérifieur

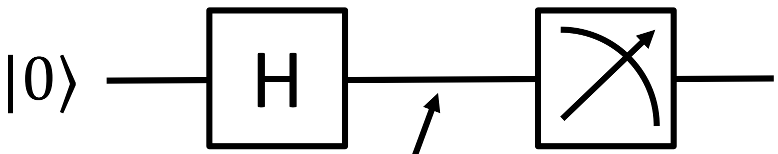
$\rightarrow (\boldsymbol{flag}, \boldsymbol{b})$

"boîte quantique"

- Le vérifieur a en tête un circuit quantique C
- Il interagit avec la "boîte quantique" à travers un canal *classique*
- Il retourne $(flag, b)$ tel que si $\Pr(flag = ACC)$ n'est pas trop petit,

$$\Pr(\ b = 1\ | flag = ACC) \quad \approx \quad \Pr(\ C \text{ retourne } 1 \text{ sur l'entrée } |0^n\rangle \ \ )$$

L'exemple le plus simple

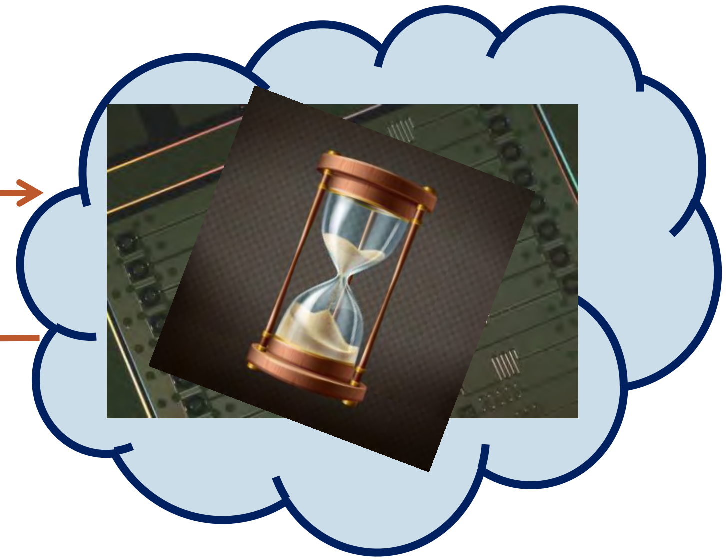


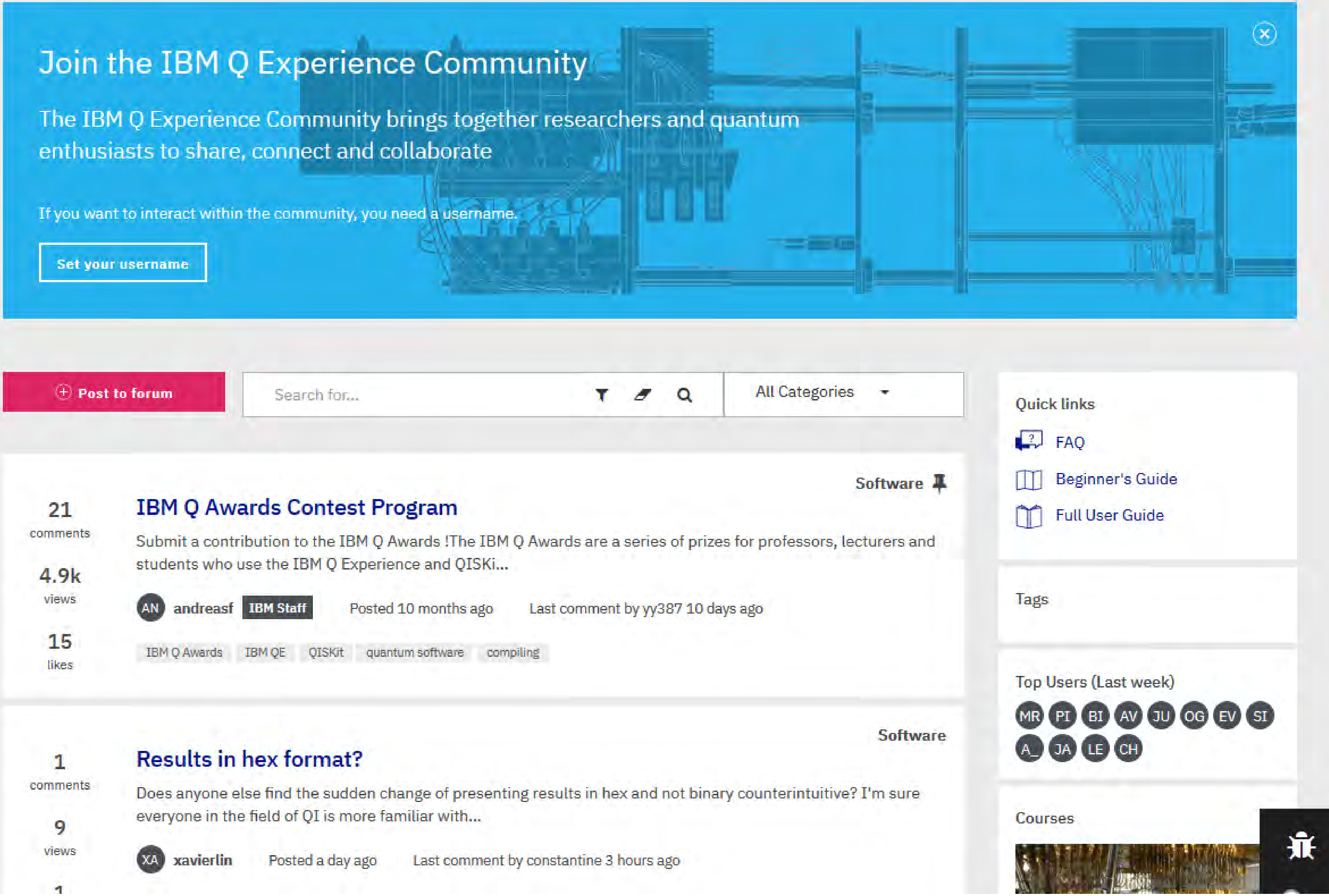
$$\begin{cases} b = 0 \text{ w.p. } 50\% \\ b = 1 \text{ w.p. } 50\% \end{cases}$$

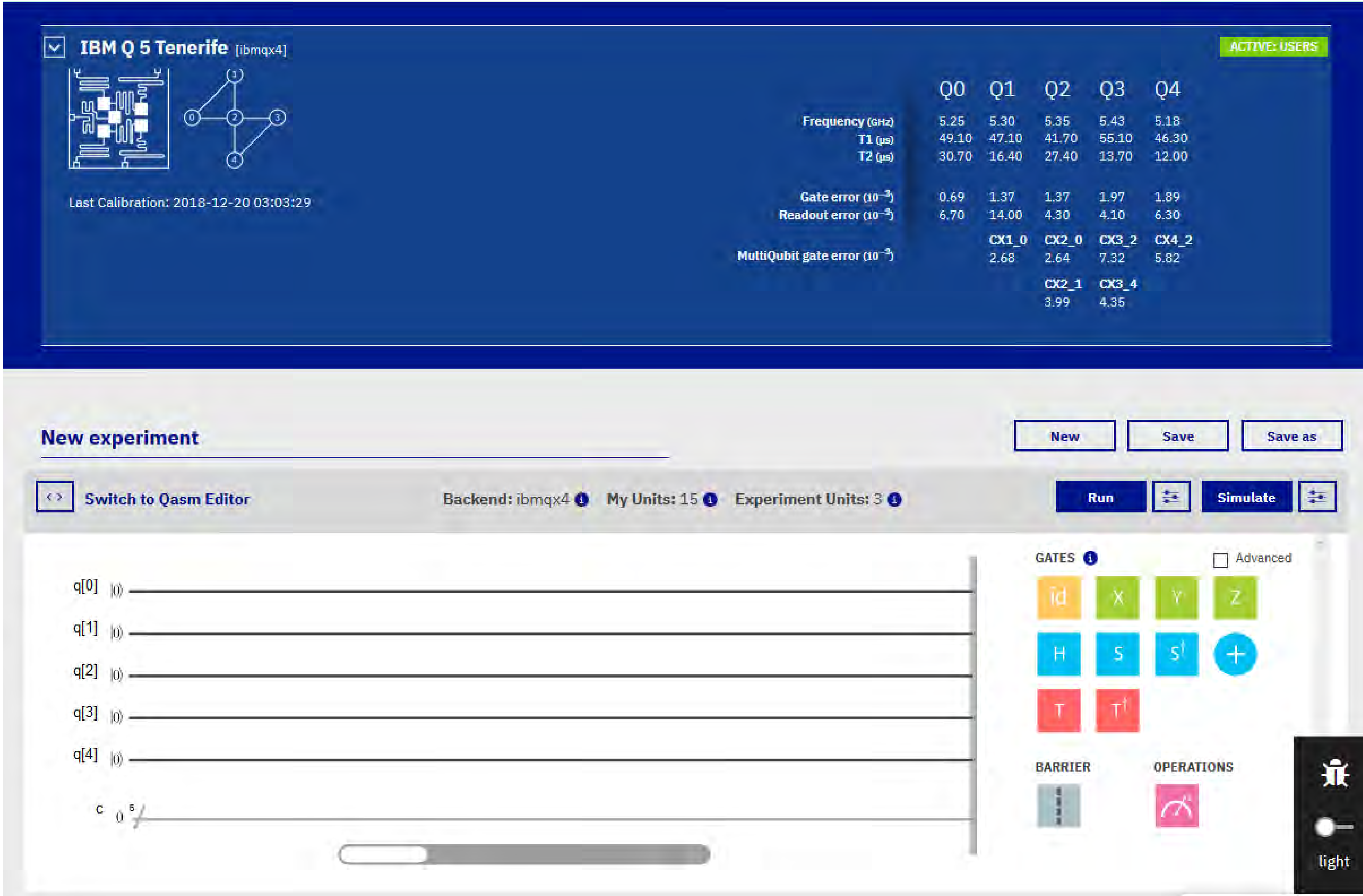
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

"description du circuit C"

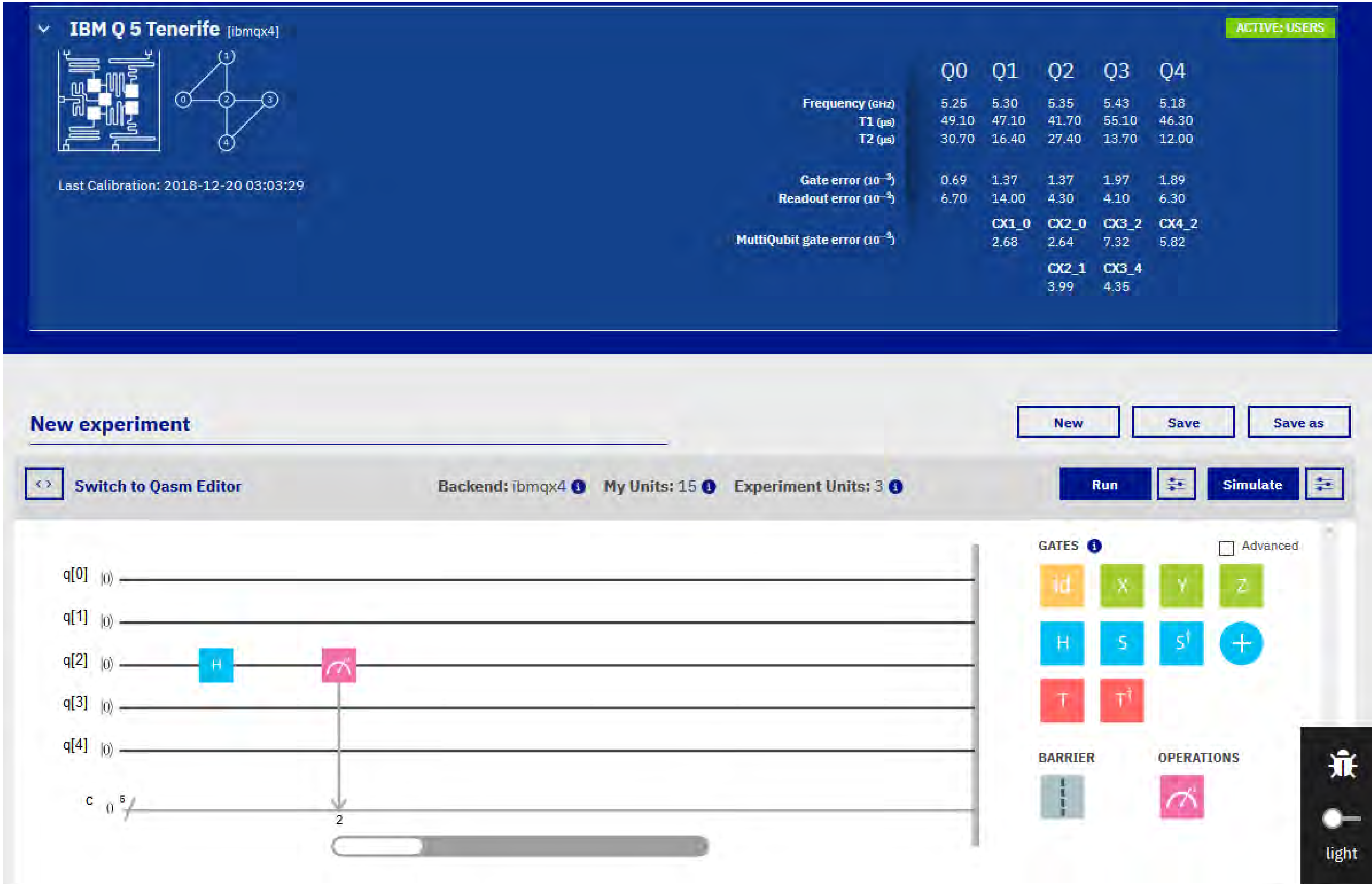
"$b = 0$"

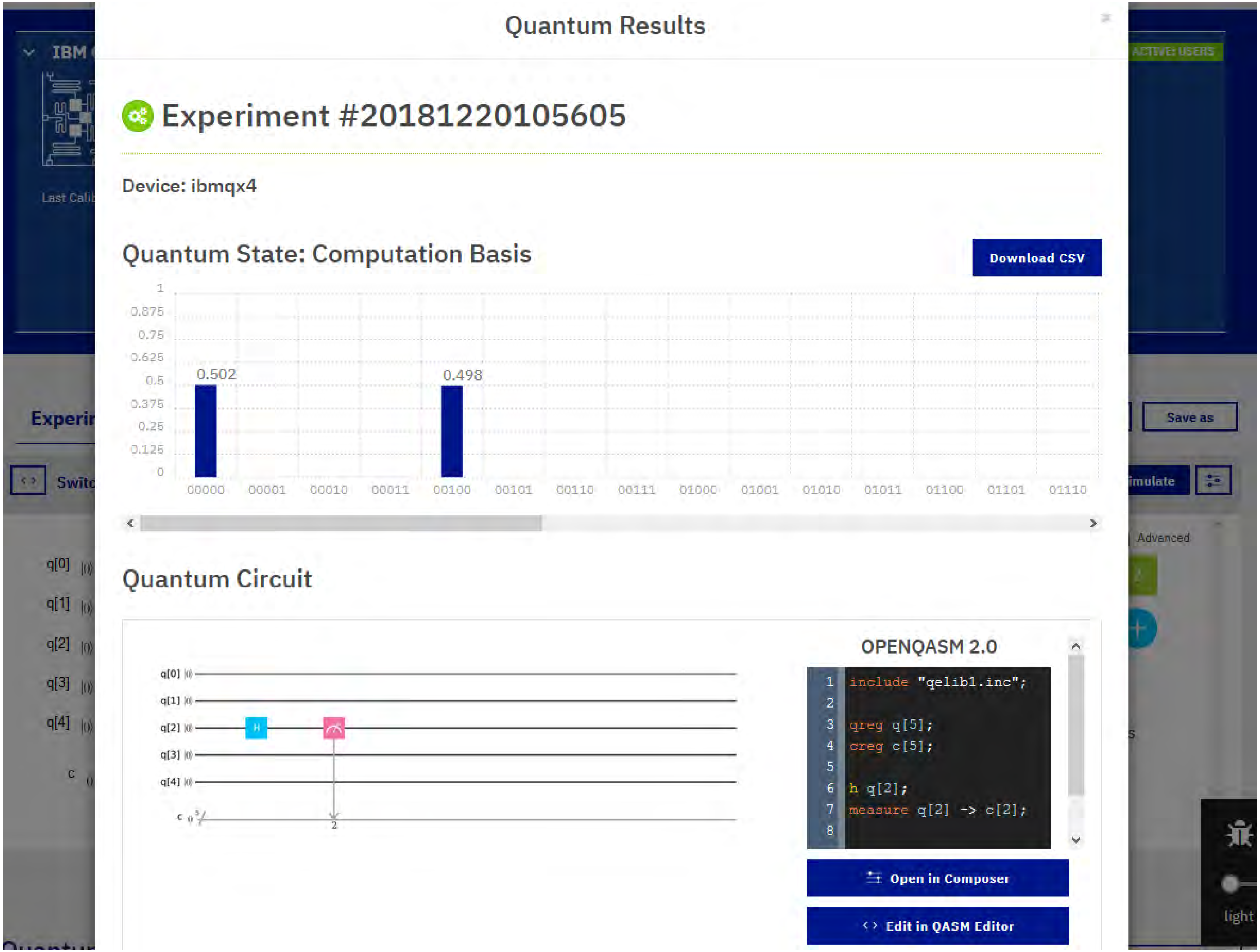



Join the IBM Q Experience Community
The IBM Q Experience Community brings together researchers and quantum enthusiasts to share, connect and collaborate
If you want to interact within the community, you need a username.
Set your username
Post to forum
Search for...
All Categories
Quick links
FAQ
Beginner's Guide
Full User Guide
Tags
Top Users (Last week)
MR PI BI AV JU OG EV SI A_ JA LE CH
Courses
Software
21 comments
4.9k views
15 likes
IBM Q Awards Contest Program
Submit a contribution to the IBM Q Awards !The IBM Q Awards are a series of prizes for professors, lecturers and students who use the IBM Q Experience and QISKi...
AN andreasf IBM Staff
Posted 10 months ago
Last comment by yy387 10 days ago
IBM Q Awards
IBM QE
QISKit
quantum software
compiling
Software
1 comments
9 views
Results in hex format?
Does anyone else find the sudden change of presenting results in hex and not binary counterintuitive? I'm sure everyone in the field of QI is more familiar with...
XA xavierlin
Posted a day ago
Last comment by constantine 3 hours ago

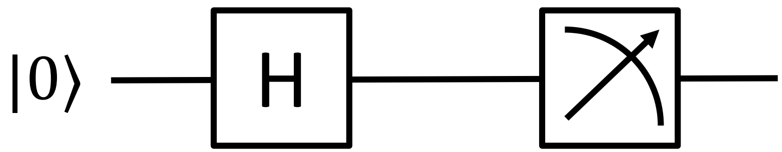


IBM Q 5 Tenerife [ibmqx4]
ACTIVE: USERS
Last Calibration: 2018-12-20 03:03:29
Q0 Q1 Q2 Q3 Q4
Frequency (GHz) 5.25 5.30 5.35 5.43 5.18
T1 (µs) 49.10 47.10 41.70 55.10 46.30
T2 (µs) 30.70 16.40 27.40 13.70 12.00
Gate error (10⁻³) 0.69 1.37 1.37 1.97 1.89
Readout error (10⁻²) 6.70 14.00 4.30 4.10 6.30
MultiQubit gate error (10⁻²)
CX1_0 2.68
CX2_0 2.64
CX3_2 7.32
CX4_2 5.82
CX2_1 3.99
CX3_4 4.35
New experiment
New
Save
Save as
Switch to Qasm Editor
Backend: ibmqx4
My Units: 15
Experiment Units: 3
Run
Simulate
q[0] |0⟩
q[1] |0⟩
q[2] |0⟩
q[3] |0⟩
q[4] |0⟩
c 0 5
GATES
Advanced
id X Y Z
H S S†
T T†
BARRIER
OPERATIONS
light

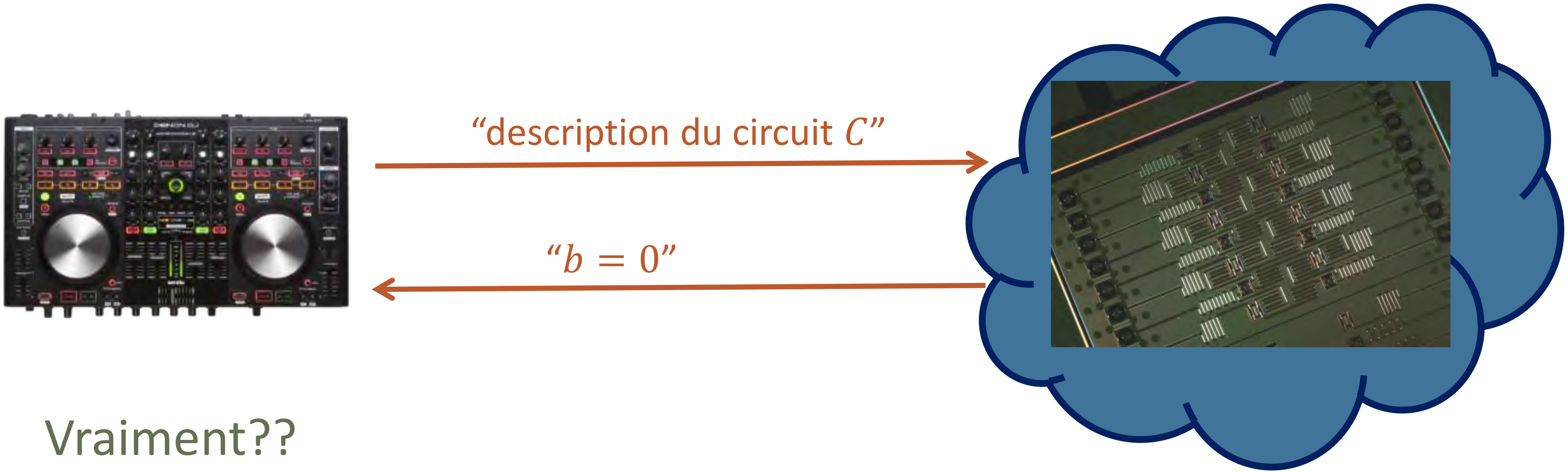

IBM Q 5 Tenerife [ibmqx4]
ACTIVE: USERS
Last Calibration: 2018-12-20 03:03:29
Q0 Q1 Q2 Q3 Q4
Frequency (GHz) 5.25 5.30 5.35 5.43 5.18
T1 (µs) 49.10 47.10 41.70 55.10 46.30
T2 (µs) 30.70 16.40 27.40 13.70 12.00
Gate error (10^-3) 0.69 1.37 1.37 1.97 1.89
Readout error (10^-3) 6.70 14.00 4.30 4.10 6.30
MultiQubit gate error (10^-3)
CX1_0 2.68
CX2_0 2.64
CX3_2 7.32
CX4_2 5.82
CX2_1 3.99
CX3_4 4.35
New experiment
New
Save
Save as
Switch to Qasm Editor
Backend: ibmqx4
My Units: 15
Experiment Units: 3
Run
Simulate
q[0]
q[1]
q[2]
q[3]
q[4]
c
H
2
GATES
Advanced
id
X
Y
Z
H
S
T
BARRIER
OPERATIONS
light


Quantum Results
Experiment #20181220105605
Device: ibmqx4
Quantum State: Computation Basis
Download CSV
1
0.875
0.75
0.625
0.5
0.375
0.25
0.125
0
0.502
0.498
00000
00001
00010
00011
00100
00101
00110
00111
01000
01001
01010
01011
01100
01101
01110
Quantum Circuit
q[0]
q[1]
q[2]
q[3]
q[4]
H
c
2
OPENQASM 2.0
include "qelib1.inc";
qreg q[5];
creg c[5];
h q[2];
measure q[2] -> c[2];
Open in Composer
Edit in QASM Editor
Save as
Advanced
light

L’exemple le plus simple



$$\begin{cases} b = 0 \text{ w.p. } 50\% \\ b = 1 \text{ w.p. } 50\% \end{cases}$$



Vraiment??

Répéter et faire une analyse statistique?

Certification d'aléas sous hypothèse d'isolation spatiale

Non-localité quantique

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. Einstein, B. Podolsky and N. Rosen, *Institute for Advanced Study, Princeton, New Jersey*

III.5 ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

John S. Bell†

THE paradox of Einstein, Podolsky a
could not be a complete theory but sh
ables were to restore to the theory ca
mathematically and shown to be inco
the requirement of locality, or more p
by operations on a distant system wi
ficulty. There have been attempts [3
ment no "hidden variable" interpreta
examined elsewhere [4] and found wa
tum theory [5] has been explicitly co
local structure. This is characterist
reproduces exactly the quantum mech

PROPOSED EXPERIMENT TO TEST LOCAL HIDDEN-VARIABLE THEORIES*

John F. Clauser†
Department of Physics, Columbia University, New York, New York 10027

and

Michael A. Horne
Department of Physics, Boston University, Boston, Massachusetts 02215

and

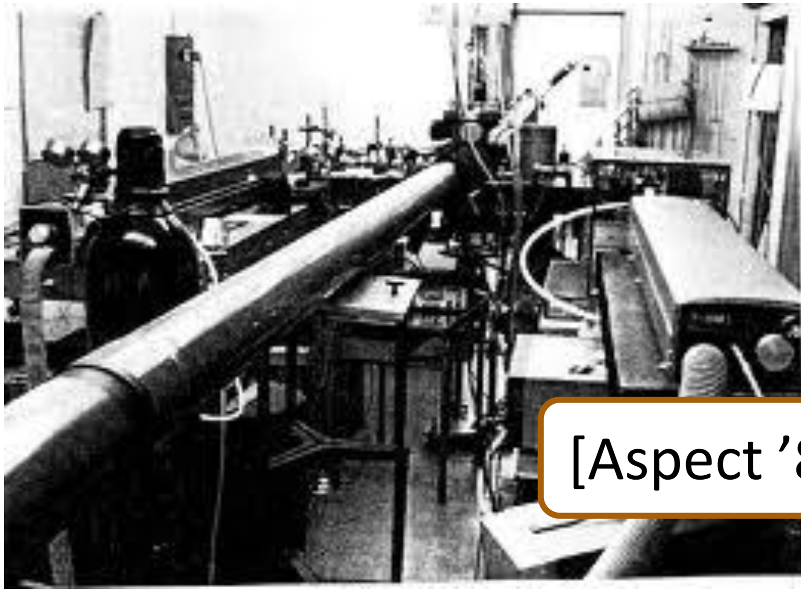
Abner Shimony
Departments of Philosophy and Physics, Boston University, Boston, Massachusetts 02215

and

Richard A. Holt
Department of Physics, Harvard University, Cambridge, Massachusetts 02138
(Received 4 August 1969)

A theorem of Bell, proving that certain predictions of quantum mechanics are inconsistent with the entire family of local hidden-variable theories, is generalized so as to apply to realizable experiments. A proposed extension of the experiment of Kocher and Commins, on the polarization correlation of a pair of optical photons, will provide a decisive test between quantum mechanics and local hidden-variable theories.

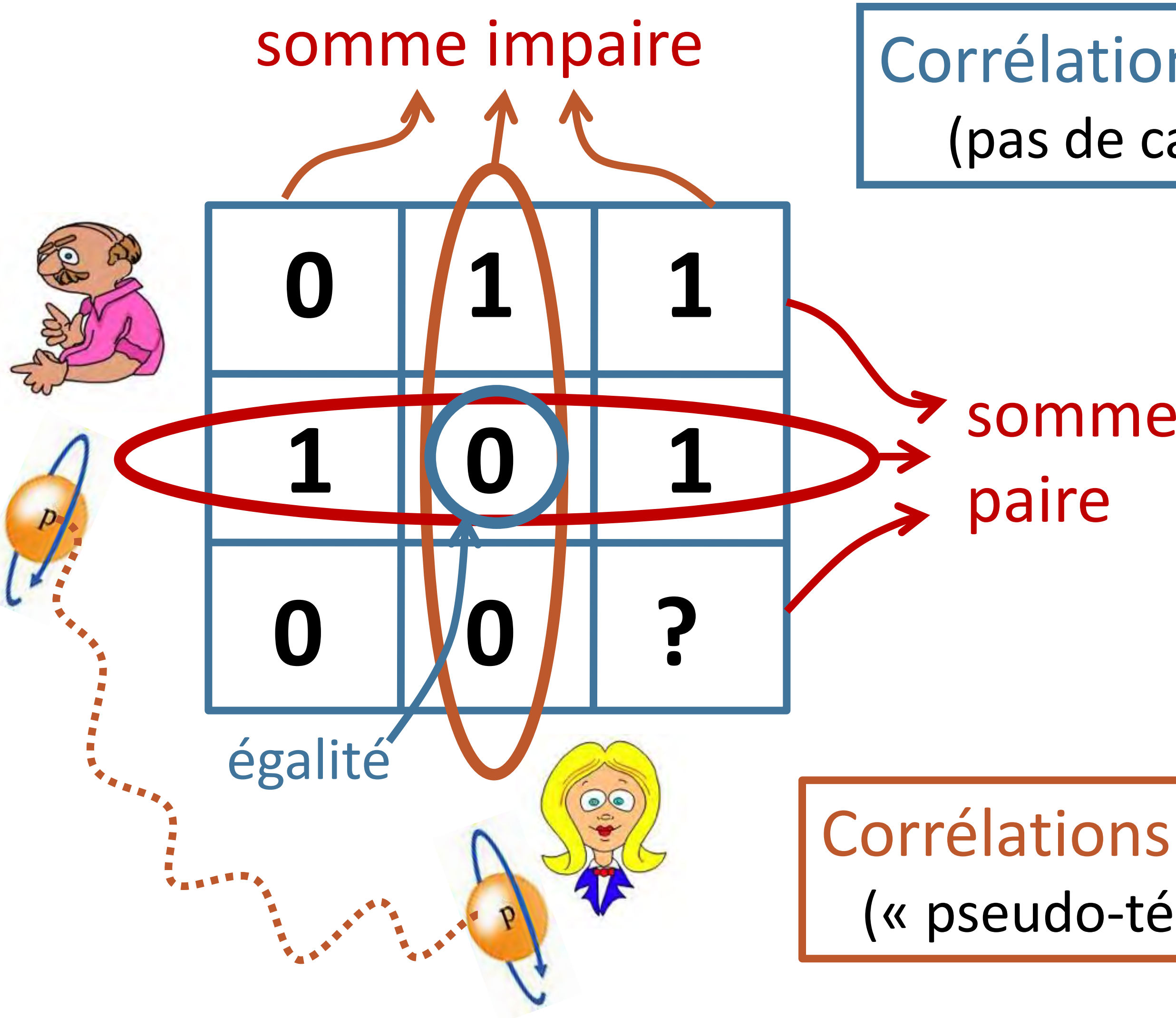
Non-localité quantique



[Aspect '82]

[Hansen'16]

Le Carré Magique de Mermin-Peres



Corrélations classiques: p_s=8/9
(pas de carré magique parfait!)

Corrélations quantiques: p_s^* =1!
(« pseudo-télépathie » quantique)

Le Carré Magique de Mermin-Peres

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

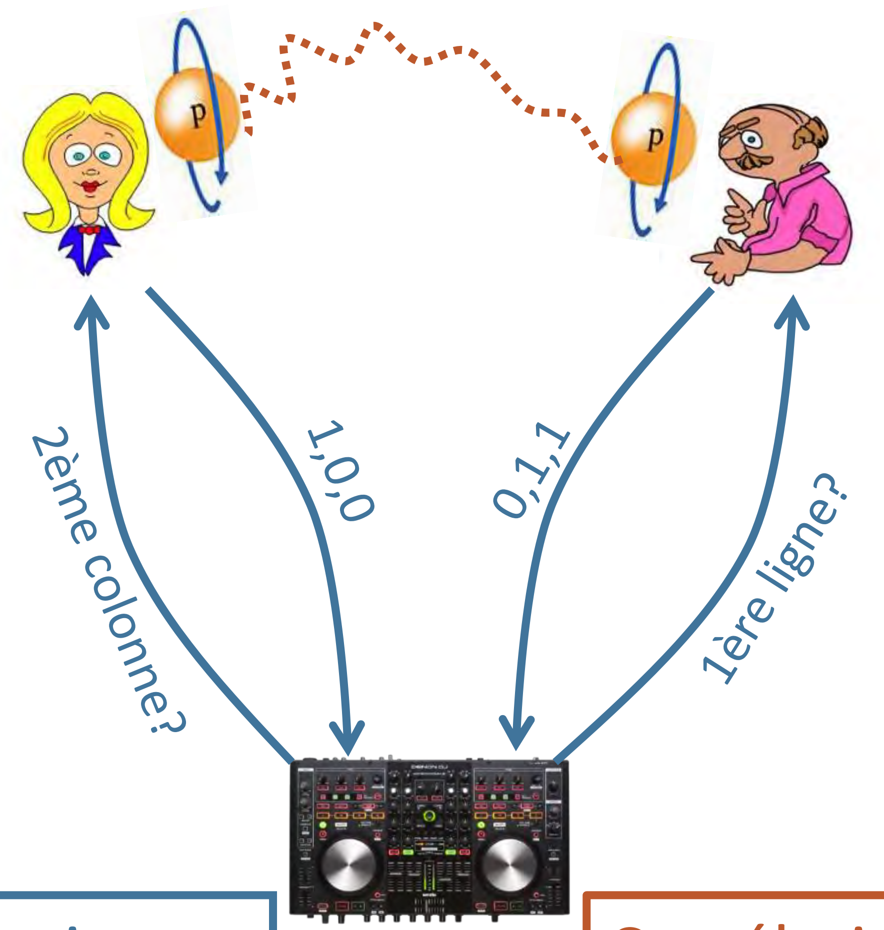
$$Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

Produit -1

$I \otimes Z$	$Z \otimes I$	$Z \otimes Z$
$X \otimes I$	$I \otimes X$	$X \otimes X$
$-X \otimes Z$	$-Z \otimes X$	$Y \otimes Y$

Produit $+1$

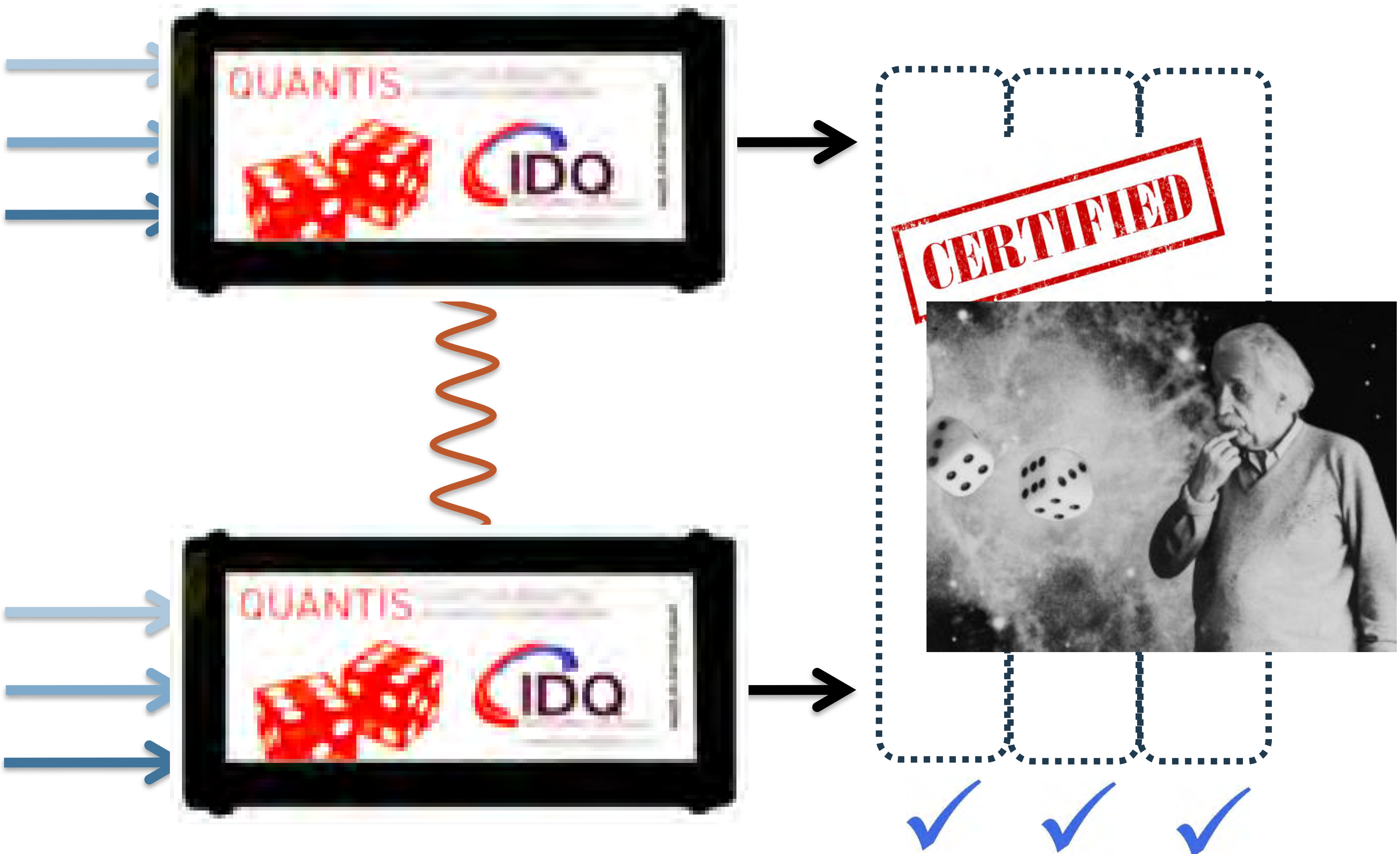
Le Carré Magique de Mermin-Peres



Corrélations classiques:
$p_s=8/9$

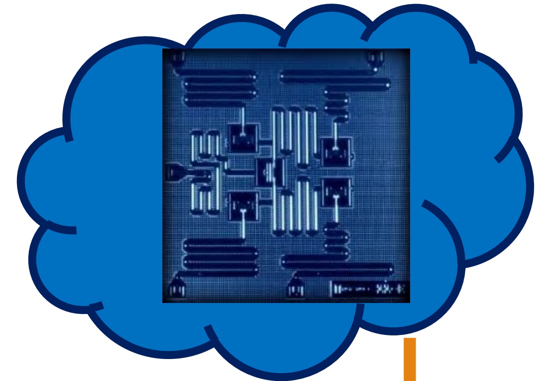
Corrélations quantiques:
$p_s^*=1!$

Génération d’aléas certifié



Certification d'aléas sous hypothèse calculatoire

Tests sous hypothèses calculatoires



- Le vérifieur est classique, temps polynomial
- Le serveur est quantique(?), temps polynomial
- Hypothèse: il existe un problème calculatoire difficile pour tous: classique, quantique, vérifieur, serveur

Processus quantique(?)

LWE: Étant donnée $A \in \mathbb{Z}_q^{m \times n}$ et $u = As + e$
où $u \leftarrow_R \mathbb{Z}_q^n$ et $e \leftarrow_\chi \mathbb{Z}_q^m$ est “petit”, trouver u

Vérifieur

Trouver un avantage pour le quantique

- Algorithme de Simon: $f: \{0,1\}^n \rightarrow \{0,1\}^n$ telle que f est 2-à-1
  - Superposition uniforme sur $|x\rangle$, évaluation de f et mesure d'une image y:

$$\frac{1}{\sqrt{2}}|x_0\rangle + \frac{1}{\sqrt{2}}|x_1\rangle$$

  - Transformée de Fourier quantique: d tel que $d \cdot (x_0 \oplus x_1) = 0$

- Aucune f concrete connue ne donne un avantage exponentiel

Soit $f: \{0,1\}^n \rightarrow \{0,1\}^n$ telle que f est 2-à-1 et:

- Il est difficile de trouver un triple (x_0, x_1, y) t.q. $f(x_0) = f(x_1) = y$
- Il est difficile de trouver $(x_0$ ou $x_1)$ *et* $(d \neq 0$ s.t. $d \cdot (x_0 \oplus x_1) = 0\,)$

Certification d'aléas sous hypothèse calculatoire

Vérifieur

f →

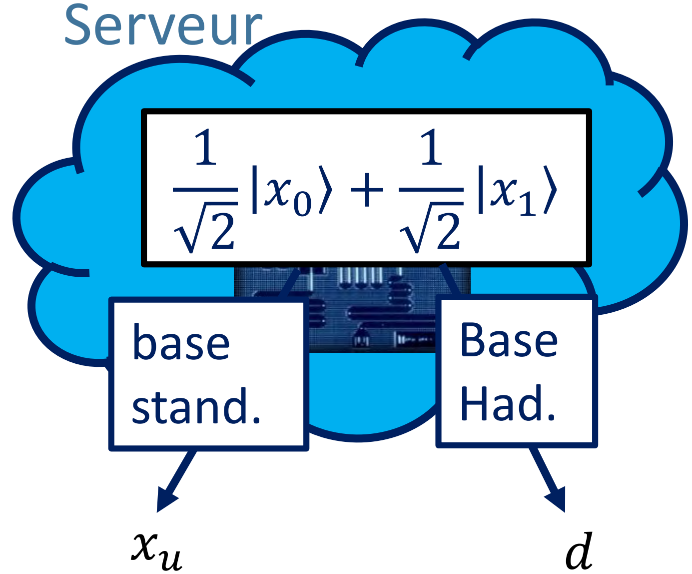
← *image* y

challenge $c = 0/1$ →

← $c = 0$: x_0 ou x_1

$c = 1$: d t.q. $d \cdot (x_0 \oplus x_1) = 0$

Serveur



- Hypothèse calculatoire: aucun processus en temps polynomial ne peut *simultanément* obtenir une réponse correcte aux deux challenges

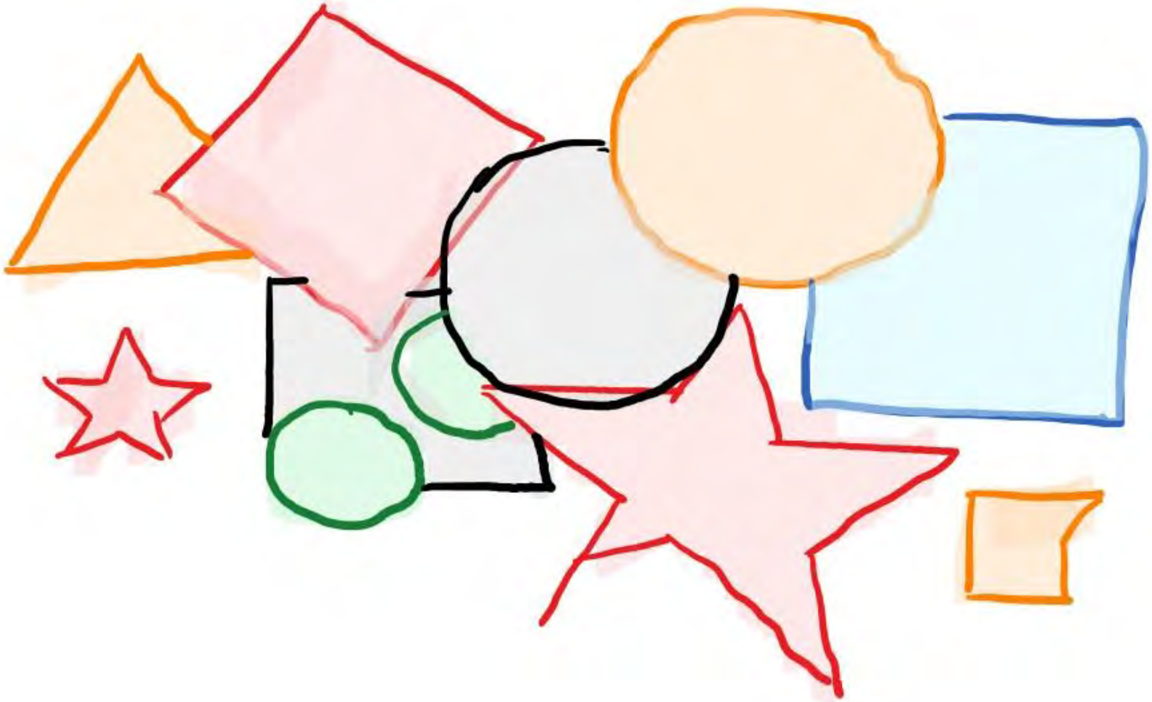
- Succès pour $c = 1$ → état déterminé pour $c = 1$
  → generation d'aléas pour $c = 0$
- Principe d'incertitude calculatoire!

Soit $f: \{0,1\}^n \rightarrow \{0,1\}^n$ telle que f est 2-à-1 et:

- Il est difficile de trouver un trio (x_0, x_1, y): $f(x_0) = f(x_1) = y$
- Il est difficile de trouver $(x_0$ ou $x_1)$ *et* $(d \neq 0$ s.t. $d \cdot (x_0 \oplus x_1) = 0\ )$

Conclusions

- Deux hypothèse possibles: isolation spatiale / limitation calculatoire
- Non-localité / “Non-rembobinage” → test du quantique + aléas certifié
- Pour aller plus loin:
  - Cryptographie: distribution de clé, calcul distribué
  - Délégation/Vérification de calculs quantiques: “quantum cloud”
- Et en pratique?
  - Génération non-locale de nombres aléatoires
  - Tests de circuits quantiques à petite échelle



Merci pour votre attention

vidick@caltech.edu

Bibliographie abrégée

Arnon-Friedman, R., Renner, R., & Vidick, T. (2019). Simple and tight device-independent security proofs. *SIAM Journal on Computing*, *48*(1), 181-225.

Brakerski, Z., Christiano, P., Mahadev, U., Vazirani, U., & Vidick, T. (2018, October). A cryptographic test of quantumness and certifiable randomness from a single quantum device. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 320-331). IEEE.

Colbeck, R. (2009). Quantum And Relativistic Protocols For Secure Multi-Party Computation. *Ph. D. Thesis*.

Mahadev, U. (2018, October). Classical verification of quantum computations. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 259-267). IEEE

Mayers, D., & Yao, A. (2004). Self testing quantum apparatus. *Quantum Information & Computation*, *4*(4), 273-286.

Pironio, S., Acín, A., Massar, S., de La Giroday, A. B., Matsukevich, D. N., Maunz, P., ... & Monroe, C. (2010). Random numbers certified by Bell's theorem. *Nature*, *464*(7291), 1021-1024.

Reichardt, B. W., Unger, F., & Vazirani, U. (2013). Classical command of quantum systems. *Nature*, *496*(7446), 456-460.

Vazirani, U., & Vidick, T. (2012, May). Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing* (pp. 61-76).

Vazirani, U., & Vidick, T. (2019). Fully device independent quantum key distribution. *Communications of the ACM*, *62*(4), 133-133.