

# FLASH



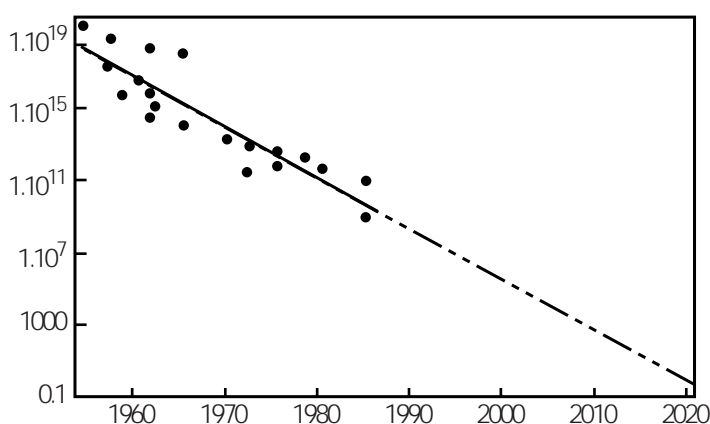
## 2021, l'Odyssée quantique

Jacqueline.Dousson@epfl.ch, SIC



Avez-vous déjà jeté un oeil sur les courbes représentant la miniaturisation des processeurs et des moyens de stockage de données (voir ci-dessous)? Une extrapolation même approximative nous montre que vers 2020, il ne nous faudra que quelques atomes pour stocker un bit. Sur un tel système, les règles classiques ne peuvent plus s'appliquer, nous sommes alors dans un autre monde où les comportements sont dictés par d'autres lois, celles de la mécanique quantique.

L'informatique quantique, née de la rencontre de physiciens et de théoriciens de l'informatique n'a pas attendu 2020 pour jeter les bases d'un nouvel espace technique. On est encore loin de réalisations de taille industrielle, mais ce domaine est suffisamment prometteur pour que l'on doive dès aujourd'hui s'y intéresser, car cela risque bien de bouleverser le paysage informatique d'ici 10 à 20 ans et avec lui quelques-unes de nos certitudes.



Nombre d'atomes nécessaires pour représenter 1 bit d'information en fonction de l'année. Dans ce mode semi-logarithmique, la droite indique qu'on a une évolution exponentielle. Par extrapolation, on en déduit que le niveau 1 atome pour 1 bit est atteint aux environs de 2020 (extrait de: Exploration in Quantum Computing, Williams & Clearwater, Springer-Verlag)

### sommaire FI 3

- 1 2021, l'Odyssée quantique
- 6 L'avenir des systèmes d'information
- 8 Offre d'emploi
- 9 LabVIEW User Group Meeting
- 14 Parlons AppleTalk
- 16 Plans EPFL
- 17 L<sup>A</sup>T<sub>E</sub>X au LEMA
- 19 Les lecteurs nous écrivent...
- 21 Ça n'arrive pas qu'aux autres...
- 23 Formation
- 27 Computer 99
- 28 Calendrier



### Prochaines parutions

	délai FI	parution FI
4	22.04.99	11.05.99
5	20.05.99	08.06.99
6	17.06.99	06.07.99
SP	01.07.99	31.08.99
7	26.08.99	14.09.99
8	30.09.99	19.10.99
9	28.10.99	16.11.99
10	25.11.99	14.12.99

## Le q-bit

Un ordinateur classique, ce sont des bits qui peuvent prendre la valeur 0 ou 1. Dans un ordinateur quantique, l'élément de base est le q-bit (quantum bit), qui peut exister dans deux états électroniques distincts. Mais, contrairement à la mécanique classique, le q-bit peut aussi présenter une superposition cohérente de ces 2 états, ce qui veut dire qu'il est à la fois dans l'état 0 et l'état 1 (voir **Le principe de superposition**). Peu importe ici que le q-bit soit représenté par le spin d'un atome, la polarisation d'un photon, ou l'état mort/vivant du pauvre chat de Schrödinger: c'est un objet quantique qui obéit aux lois de la mécanique quantique.

Imaginez un système classique à 3 bits, il peut se trouver dans une configuration parmi 8 possibles (000, 001, ... 111). Avec un système quantique à 3 q-bits, les 8 configurations sont mémorisées simultanément. Un système à N q-bits travaillera sur  $2^N$  nombres à la fois. Là où l'ordinateur classique va répéter  $2^N$  fois l'opération ou faire  $2^N$  calculs en parallèle, avec l'ordinateur quantique en une seule étape on pourra appliquer la même opération sur  $2^N$  nombres distincts.

Nul besoin d'un dessin pour imaginer le gain de temps et de mémoire que pourrait nous amener cette nouvelle technologie. Mais elle nous promet beaucoup plus que cela encore, car les vrais progrès vont venir de nouveaux algorithmes qui vont permettre de résoudre des problèmes jusqu'alors inaccessibles pour l'informatique classique.

## Le problème de la décohérence

Dans le système à N q-bits décrit très sommairement plus haut, un *petit* problème n'a pas été abordé: le problème dit de la décohérence; à cause de lui, on a longtemps cru impossible la construction d'ordinateurs quantiques. Quel est-il?

C'est tout simplement que les particularités quantiques du système, sa superposition en plusieurs états, disparaît quand il y a interaction avec le monde macroscopique; le bon sens le sait bien: une mesure ne donnera jamais une superposition mais un seul état sans ambiguïté (voir **La décohérence**).

Mais, comment isoler complètement l'ordinateur de son environnement? La solution pour contourner ce phénomène de décohérence peut venir de la physique mais aussi de l'algorithmique: ce qu'on appelle les techniques de correction d'erreurs. Inspirée de la méthode de correction classique où on utilise un bit redondant, la méthode de Peter Shor des Laboratoires de recherche AT&T que, pour des raisons évidentes, je n'expliquerai pas ici, permet de reconstruire l'état quantique exact, les espoirs envers le calcul quantique renaissent!

## La cryptographie classique mise en cause

Le temps de factorisation d'un nombre par les méthodes classiques croît exponentiellement avec le nombre de chiffres: notre confiance dans le chiffrement RSA réside dans cette exponentielle. Il faudrait un temps et un nombre d'ordinateurs beaucoup trop important pour casser un codage. Ceci est sérieusement mis en question avec l'algorithme de Peter Shor, encore lui, qui factoriserait sur un ordinateur quantique un nombre entier en un temps polynomial par rapport au nombre de chiffres; même avec peu de connaissances mathématiques, on réalise que entre exponentiel et polynomial, il y a juste de quoi inquiéter les spécialistes de la cryptographie. Rassurez-vous, nous, nous pouvons continuer à coder nos informations, car l'algorithme de

Shor est là, mais il manque encore l'ordinateur pour le mettre en place; mais pour combien de temps?

Un autre domaine, tout aussi fondamental en informatique est celui de la recherche d'un élément parmi n; classiquement, il faut en moyenne,  $n/2$  tentatives. L'algorithme de Grover lui promet qu'avec  $\sqrt{n}$  itérations, l'objet est trouvé. Avis aux développeurs de bases de données!

## Les premières réalisations d'ordinateurs quantiques

En septembre 98, les physiciens de Los Alamos ont démontré la faisabilité d'un ordinateur quantique à 3 q-bits, en contrôlant par RMN (Résonance Magnétique Nucléaire) les états de noyaux de molécules diluées dans un liquide. Bien sûr, on est encore loin de rivaliser avec les ordinateurs classiques les plus rapides et il reste de nombreux obstacles techniques à franchir, mais la voie est tracée.

## La décohérence

Le monde quantique est un monde où les objets se trouvent simultanément à plusieurs endroits: pour preuve, cette expérience qui consiste à intercaler entre une source d'atomes et un écran qui va enregistrer les impacts, une plaque percée de deux fentes. Ce que l'on observe est très étrange: vous avez une alternance de zones claires et de des zones sombres où aucun atome ne parvient (vous pouvez faire l'expérience sur Internet à l'adresse suivante <http://w3.edu.polytechnique.fr/physique/quantique/>).

Dans le langage de la mécanique quantique, on dit que chaque atome a dû se comporter comme une superposition de deux ondes ayant chacune traversé sa fente respective. Si vous remplacez les atomes par des objets plus gros (balle de ping-pong par exemple), vous n'observerez jamais cette figure dite d'interférence. Les superpositions d'états quantiques extrapolées au monde macroscopique conduisent donc à des absurdités telles que le célèbre *chat de Schrödinger* enfermé dans une boîte en compagnie d'un atome radioactif. Si l'atome se désintègre, il déclenche un mécanisme libérant un poison et tuant le chat. En dehors de toute mesure ce pauvre chat se retrouve dans une superposition quantique de deux états, le décrivant respectivement mort et vivant. Historiquement, Schrödinger avait pensé cette expérience pour mettre en difficulté le danois Niels Bohr et son interprétation dite de Copenhague qui postule que lors d'une mesure, vous avez un processus de réduction instantanée qui efface toute superpositions d'états.

Quel est donc ce mystérieux processus de réduction qui fait passer les chats vivants et morts aux chats vivants ou morts? Dans les années 80 et à partir d'un article de W.H Zurek, l'idée et les modèles de décohérence ont été émis: pour chaque expérience il faut distinguer trois sous-systèmes, qui sont, l'objet, l'appareil de mesure et l'environnement. L'interaction des systèmes macroscopiques avec leur environnement *brouille* très rapidement les superpositions. «Ainsi l'émergence des comportements classiques à partir des lois quantiques... résulterait d'un brouillage, des interférences quantiques, brouillage dû aux interactions avec l'environnement et qui se manifesterait systématiquement dans les systèmes formés d'un grand nombre de particules» soulignent S. Haroche J.M Raimond et M.Brune (La Recherche no 301, septembre 97) qui ont expérimentalement mis en évidence ce brouillage.

Quelle conséquence pour l'ordinateur quantique? Très grave, si l'on se réfère à l'article *L'ordinateur quantique: rêve ou cauchemar?* (La recherche no 292, novembre 96) où l'on peut lire «par conséquent si rien n'est fait pour corriger la décohérence, la tâche la plus ambitieuse que l'on puisse espérer sera de factoriser le nombre 15». Moins grave, si l'on en croit les derniers résultats de factorisation qui semblent montrer que les stratégies de correction d'erreurs sont en bonne voie.



## Cryptographie quantique vs cryptographie classique

Tout l'art de la cryptographie consiste à transmettre une information de telle sorte qu'elle ne soit compréhensible que par la seule personne à laquelle elle est destinée. Autrefois, c'était l'algorithme de chiffrement qui était soigneusement gardé secret. A notre époque, les algorithmes utilisés sont connus de tous; la sécurité provient du fait que pour déchiffrer un message il faut connaître la clé avec laquelle il a été chiffré. L'usage d'une seule clé a une fragilité évidente, il faut bien à un moment donné que l'émetteur et le récepteur du message échangent cette clé, et qui dit échange dit interception possible.

Le chiffrement à deux clés, une publique et une privée évite le problème d'échange de clé mais sa sécurité repose sur la grande difficulté de factoriser des grands nombres. Aujourd'hui, il faut 23 heures avec plusieurs dizaines de milliers d'ordinateurs pour casser une clef de 56 bits. Mais, le jour où les ordinateurs (quantiques par exemple) ou les mathématiciens trouveront le moyen de factoriser rapidement un grand nombre, la **cryptographie classique** aura montré ses limites. C'est alors qu'on pourra faire appel à la cryptographie quantique.

La cryptographie classique emploie des techniques mathématiques pour chiffrer les messages, la cryptographie quantique protège l'information par les lois de la physique. Elle repose sur le principe d'incertitude d'Heisenberg (voir **Le principe d'incertitude d'Heisenberg**), selon lequel la mesure d'un système quantique perturbe ce système.

Plusieurs méthodes de cryptographie quantique ont été décrites; prenons par exemple celle où 2 personnes, traditionnellement appelées Alice et Bob dans la littérature traitant de ce sujet, échangent un message qu'ils veulent garder secret. L'idée générale est que le texte du message préalablement codé sous forme de bits classiques est représenté par un ensemble de photons dont l'état quantique correspond à ces bits. Si un intrus agit sur un des photons il détruit la polarisation existante, et Alice et Bob s'en rendront compte immédiatement. La méthode permet donc de distribuer une clé secrète de façon totalement sécurisée, quelle que soit la puissance de calcul dont disposeraient les espions.

L'inconvénient majeur de ces méthodes est l'atténuation inévitable des photons par les fibres optiques où ils circulent. En effet il est interdit d'utiliser des ré-

pétiteurs qui amplifieraient le signal, car pour amplifier il faudrait connaître l'état du photon, et le connaître c'est le modifier (voir **Le principe d'incertitude d'Heisenberg**). La limite maximale théorique pourrait être de 50 km de fibre optiques.

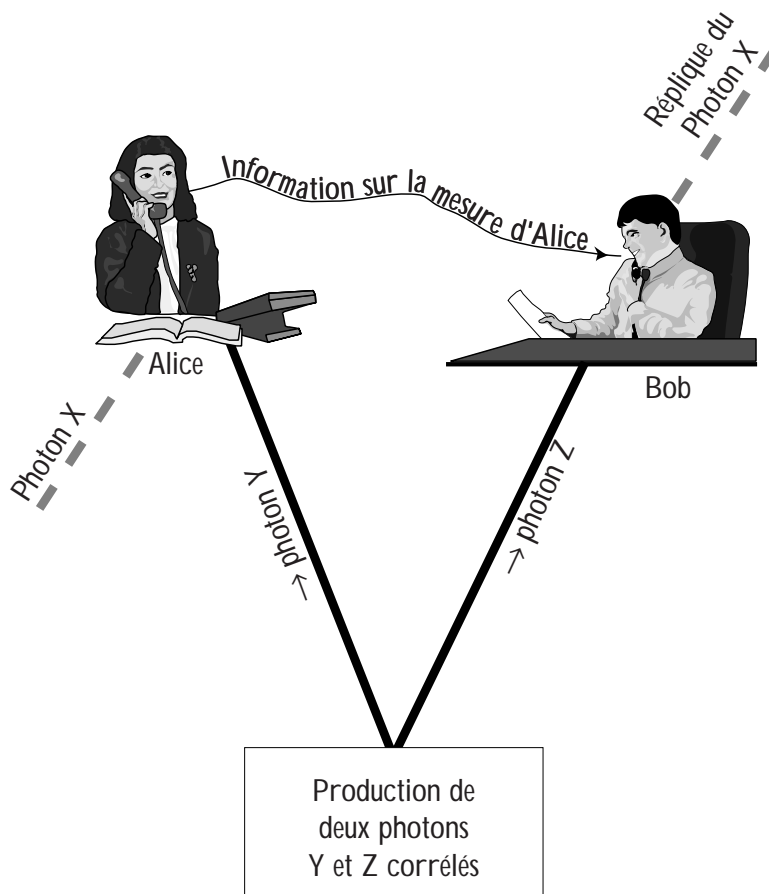
Des réalisations expérimentales de cryptographie quantique ont été réalisées par des physiciens de l'Université de Genève récemment sur une fibre optique de 23 km, ce qui est extrêmement prometteur.

### Le principe d'incertitude d'Heisenberg

Ce principe est appelé à tort d'*incertitude* car il ne s'agit pas d'incertitude de mesure au sens classique du terme. Un état quantique est constitué de plusieurs paramètres, par exemple la position et la vitesse d'une particule. Le principe d'Heisenberg stipule que si l'on mesure avec précision un paramètre (la vitesse par exemple), l'état quantique de la particule est perturbé. Ceci entraîne aussi le fait qu'on ne peut *cloner* une particule, car on ne peut jamais connaître complètement son état quantique.

### Téléportation quantique

Ce mot évoque en général des personnages de science-fiction qui peuvent être transportés d'un espace à une autre grâce aux formules d'un savant éclairé. Ici, c'est peut-être un peu moins spectaculaire à première vue, mais ne manque pas d'intérêt. Il ne s'agit pas de faire voyager des atomes mais de l'information inconnue à la vitesse de la lumière. Retrouvons Alice et Bob. Alice ne sait pas où est Bob mais veut lui transmettre l'état quantique d'un photon X, qu'elle ne connaît pas elle-même (en effet, si elle cherchait à le connaître, elle modifierait l'état quantique de X; voir **Le principe d'incertitude d'Heisenberg**). On donne à Alice et Bob 2 photons corrélés (voir **Les photons corrélés**): Y et Z. Bob emmène avec lui le photon Z. Alice fait inter-



agir X avec Y, elle envoie le résultat à Bob par des méthodes classiques de communication; jusque là rien d'extraordinaire. Quand Bob reçoit cette information, il peut opérer une transformation sur Z qui met Z dans l'état quantique de X. L'état quantique de X a donc été transporté de Alice à Bob.

En 1993, une équipe des laboratoires de recherche d'IBM a réalisé la téléportation d'un état quantique inconnu entre 2 points distincts. Ce résultat anima les milieux concernés, la téléportation sortait du domaine de la science-fiction pour devenir une réalité.

## Conclusion

IBM, Stanford, Los Alamos, ATT, ces quelques noms cités dans l'article devraient suffire à nous convaincre que le sujet est pris très au sérieux par des intérêts qui ne sont pas qu'académiques. En effet, cryptographie, vitesse de factorisation, sont des sujets très actuels au vu des énormes besoins de sécurisation de l'information transportée sur les réseaux. Et, même si l'ordinateur qui tiendrait dans quelques gouttes de liquide ne voit jamais le jour, parions sans trop de risques, que l'informatique quantique n'a pas fini de nous étonner. Rendez-vous en 2021!

## Quelques livres, pages web, articles, FAQ

Livres:

- A tout seigneur tout honneur **R.P. Feynman**, *Lectures on Computation*, Addison-Wesley, 1996.  
Regard d'un physicien pour des étudiants en *computer science*. A ne pas manquer les chapitres 5 et 6 (*Reversible Computation and the Thermodynamics of Computing, Quantum Mechanical Computers*)
- **Colin P. Williams, Scott H. Clearwater**, *Explorations in quantum computing*, Springer-Verlag, 1997.  
C'est un livre très complet sur la question avec un CDROM d'exemples écrits en Mathematica.
- **David Deutsch**, *The Fabric of Reality*, Penguin Books, 1997.  
Livre étrange de celui qui a décrit en 85 la première machine de Turing quantique.

Web:

- Le cours de *quantum computation* (Physics 229), [www.theory.caltech.edu/people/preskill/](http://www.theory.caltech.edu/people/preskill/)
- Un autre cours de **Samuel L. Braunstein**: [chemphys.weizmann.ac.il/~schmuel/comp/comp.html](http://chemphys.weizmann.ac.il/~schmuel/comp/comp.html)

- **Claude Crépeau** (qui fit partie de l'équipe d'IBM qui a réalisé la première expérience de téléportation en 93): [www.cs.mcgill.ca/~crepeau/index.html](http://www.cs.mcgill.ca/~crepeau/index.html)
- **Peter Shor**: [www.research.att.com/~shor/](http://www.research.att.com/~shor/)
- The Stanford-Berkeley-MIT-IBM, *NMR Quantum Computing Project*: [squint.stanford.edu/](http://squint.stanford.edu/)

■ Quantum information and quantum computation at IBM: [www.research.ibm.com/quantuminfo/](http://www.research.ibm.com/quantuminfo/)

■ à l'Université de Genève, le Groupe de Physique Appliquée: [www.unige.ch/gap](http://www.unige.ch/gap)

Articles:

■ Scientific American, *Quantum Computing with Molecules*: [www.sciam.com/1998/0698issue/0698gershenfeld.html](http://www.sciam.com/1998/0698issue/0698gershenfeld.html) (voir aussi **Pour la Science** d'août 1998)

■ Des pages de référence sur le site de Los Alamos: [xxx.lanl.gov/](http://xxx.lanl.gov/)

[archive/quant-ph](http://archive/quant-ph),

- par exemple: quant-ph/9809019: E. Rieffel, W. Polak, *An Introduction to Quantum Computing for Non-Physicist*
- quant-ph/9812037: Dorit Aharonov, *Quantum Computation*.

FAQ:

- Quantum computing FAQ: [www.rdrop.com/~cary/html/quantum\\_c\\_faq.html](http://www.rdrop.com/~cary/html/quantum_c_faq.html) ■

## Flash informatique

Les articles accompagnés du tampon officiel engagent l'unité, les autres ne reflètent que l'opinion de leurs auteurs. Toute reproduction, même partielle, n'est autorisée qu'avec l'accord de la rédaction et des auteurs.

Rédacteur en chef: Jacqueline Dousson, [fi@epfl.ch](mailto:fi@epfl.ch)

Mise en page et graphisme: Appoline Raposo de Barbosa  
Comité de rédaction: Jean-Daniel Bonjour, Jean-Michel Chenais, Milan Crvcenin, Laurent Desimone, Jean-Jacques Dumont, Pierre-André Haldy, Catherine Jean-Pousin, Hervé Le Pezenec, François Roulet, Christophe Salzmann & Jacques Virchaux  
Impression: Atelier de Reprographie EPFL  
Tirage: 4000 exemplaires

Adresse Web: <http://sawwww.epfl.ch/SIC/SA/publications/>

Adresse: SIC-SA EPFL, CP 121, CH-1015 - Lausanne

Téléphone: +41 (21) 693 22 46 & 22 47



ISSN 1420-7192 9 771420 719001