INSTITUT DE FRANCE
Académie des sciences

Conférence débat de l'Académie des sciences

CALCUL, INFORMATIQUE & ORDINATEURS QUANTIQUES

Mardi 2 avril 2013 de 14h00 à 17h00

Organisateur :
Roland GLOWINSKI
Membre de l'Académie des sciences

Académie des sciences

Grande salle des séances

Palais de l'Institut de France

23, quai de Conti
75006 Paris

14 h 00 **Introduction**
Roland GLOWINSKI, *Membre de l'Académie des sciences*

14 h 15 **Introduction au Traitement Quantique de l'Information**
Philippe GRANGIER, *Institut d'Optique, Palaiseau*

14 h 45 **Mathematical Aspect of Quantum Computation**
Reinhard WERNER, *University of Hanover*

15 h 15 **Des Circuits Supraconducteurs pour l'Information Quantique**
Daniel ESTÈVE, *Quantronics, SPEC, CEA-Saclay, Membre de l'Académie des sciences*

15 h 45 **Secure Quantum Cloud Computing**
Elham KASHEFI, *University of Edinburgh*

16 h 15 **Discussion générale et conclusion**

Contact : Académie des sciences – Institut de France
Service des séances – sandrine.chermet@academie-sciences.fr

Introduction
Sur le calcul, l'informatique et les ordinateurs quantiques

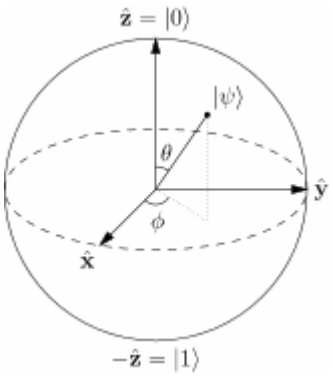
Roland GLOWINSKI, *Membre de l'Académie des sciences*

Le ***Calcul***, l'***Informatique*** et les ***Ordinateurs Quantiques*** forment l'essentiel de ce que les Anglo-Saxons désignent sous le vocable unique de ***Quantum Computing*** (QC). Le principe général du QC est de tirer parti des lois et phénomènes (parfois surprenants pour les non-spécialistes) de la ***Mécanique Quantique*** pour le ***Traitement de l'Information***; parmi ces lois et phénomènes, nous mentionnerons la ***superposition*** et l'***enchevêtrement*** (intrication) quantiques.

Bien que le QC en soit encore au stade de l'enfance, les possibilités (largement théoriques pour l' instant) qu'il offre de pouvoir résoudre, dans des temps de calcul raisonnables, des problèmes non-solubles par les ordinateurs digitaux actuels (et ceux à venir dans les prochaines décennies) en ont fait un thème de recherches très actives en Europe, aux USA, en Chine, en Australie, etc. Parmi ces problèmes difficiles, il convient de mentionner ceux qui relèvent des sciences du cryptage, ce qui explique l'intérêt porté au QC par de nombreux organismes civils et militaires, publics et privés, et les recherches mentionnées ci-dessus.

Compte tenu de l'émergence de cette discipline, encore assez peu connue du grand public, et même de nombre de scientifiques, l'Académie des Sciences a pris l' initiative d'organiser, le 2 Avril 2013, à l'Académie, 23 Quai de Conti à Paris, une session ouverte au public, spécialement dédiée au Calcul, à l' Informatique et aux Ordinateurs Quantiques. Lors de cette session, quatre spécialistes du QC aborderont les thèmes suivants:

- Bases Physique du QC.
- Bases Mathématiques du QC.
- La Circuiterie du QC.
- Aspects Algorithmiques du QC.



On a visualisé ci-dessus la ***Sphère de Bloch ;*** cet 'objet', sans doute le plus emblématique du QC, fournit une représentation géométrique du circuit logique élémentaire à la base des ordinateurs quantiques. Elle porte le nom de ***Felix Bloch*** (1905-1983), Prix Nobel de Physique en 1952 pour ses travaux sur le Magnétisme Nucléaire.

Introduction au Traitement Quantique de l'Information

Philippe GRANGIER, *Institut d'Optique, Palaiseau*

Dans cet exposé je présenterai les concepts fondamentaux du traitement quantique de l'information : les bits quantiques (qubits), les registres quantiques, les portes logiques quantiques, en soulignant en quoi la physique quantique les rend fondamentalement différents de leurs équivalents classiques. Le principe de l'algorithme de Shor sera utilisé comme exemple, et une vue d'ensemble de l'état de l'art expérimental sera présentée.

Mathematical Aspect of Quantum Computation

Reinhard WERNER, *University of Hanover*

Quantum computers, once they are built, are expected to outperform all classical computers, even those of the future. I will explain the meaning of this absurdly bold seeming claim by briefly reviewing the notion of computational complexity. This shows that a purely classical notion of computation misses some of the options we have for building real computational devices. I will then describe the missing elements in intuitive terms and in the mathematical language of quantum information theory. Comparing the basic quantum computer architectures I will then discuss why it is so hard to pinpoint the origin of quantum speedups, and how a quantum extension of the Church-Turing thesis might be stated and, perhaps, proved.

Des Circuits Supraconducteurs pour l'Information Quantique

Daniel ESTÈVE, *Quantronics, SPEC, CEA-Saclay*
Membre de l'Académie des Sciences

Des circuits électriques "à l'état solide" se comportant comme des atomes artificiels sont développés actuellement pour le traitement quantique de l'information. Après une introduction générale aux bits quantiques (qubits) supraconducteurs, je décrirai des expériences utilisant le "transmon", un dispositif directement inspiré par les expériences d'électrodynamique quantique qui utilisent de vrais atomes en cavité. Je décrirai le fonctionnement d'un processeur élémentaire qui démontre l'accélération d'un algorithme quantique, et je présenterai des structures hybrides, dans lesquelles sont combinés des qubits supraconducteurs et des entités microscopiques, par exemple des spins.

Secure Quantum Cloud Computing

Elham KASHEFI, *University of Edinburgh*

Although vast technological developments already allow for small-scale quantum computers, the hurdles encountered in realising quantum devices are enormous. This intrinsic technical complexity may result in, initially, only a few powerful quantum computers. Obviously, a key challenge in using such central quantum computers is enabling a quantum computation on a remote untrusted server, while keeping the clients data hidden from the server. The classical analogue of this issue (computing with encrypted data without decryption) was addressed for the first time in 1978 by Rivest, Adleman, and Dertouzos, called fully homomorphic encryption (FHE) scheme and became one of the most active fields in cryptography leading to secure voting systems, collision-resistant hash functions, private information retrieval schemes and secure cloud computing by ensuring the confidentiality of processed data. A full classical solution was proposed 30 years later, in STOC 2009 by Gentry. The scheme provides only computational security and despite various improvements since then, all the existing proposals still remain too computationally demanding to be useful in practice. At the same time in FOCS 2009 we presented a simple quantum scheme (Universal Blind Quantum Computing) and showed that quantum computers can provide unconditional security in data processing. We recently achieved the first experimental demonstration of blind quantum computing (BQC), demonstrating various blind delegated computations, including the Deutsch and Grover algorithms. Remarkably, the client only needs to be able to prepare and transmit individual photonic qubits.