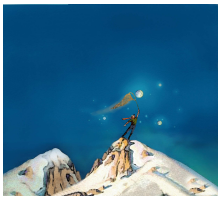

printemps des sciences
Avec le soutien de la Ministre de l'Enseignement supérieur et de la Recherche scientifique

Sciences extrêmes 19 - 25 mars 2007

ULB

L'ALGORITHMIQUE QUANTIQUE

Ben Taieb Souhaib
Département d'Informatique

Au début des années 80, Richard Feynman, Prix Nobel de Physique, suggéra d'utiliser la physique quantique au lieu de la physique classique pour faire du calcul. Quelques années plus tard, on voyait apparaître les premiers résultats, au début théoriques et ensuite expérimentaux.

En 1994, Peter Shor montre qu'on peut utiliser le calcul quantique pour factoriser un nombre entier. Cet algorithme est important car de nombreux cryptosystèmes à clés publiques, tels que RSA, deviendraient cassables, s'il était un jour programmé sur un ordinateur quantique de taille convenable.

En 1995, Lov Grover a trouvé un algorithme quantique de recherche, qui permet de faire une recherche dans une base de données en $O(\sqrt{N})$ alors qu'avec l'algorithmique classique, on le fait en $O(N)$ ou $O(\log N)$.

D'un point de vue expérimental, ce n'est qu'en 1998 qu'IBM propose un calculateur quantique à 2 qubits. Plus tard, en 2001, IBM factorisera le nombre 15, avec l'algorithme de Shor, en utilisant un calculateur quantique à 7 qubits.

Mais d'où provient cette rapidité ?

L'informatique quantique doit beaucoup à la « superposition d'états » . En effet, un bit quantique (ou qubit) peut se trouver dans deux états simultanément; ainsi, si on fait une transformation sur ce qubit, on aura appliqué la transformation aux deux états. On voit donc apparaître un certain parallélisme, qui donne à l'informatique quantique une force de calcul incroyable !

Oui, mais le calcul en parallèle existe aussi en informatique classique, non ? Il suffit d'utiliser des processeurs en parallèle ?

Bien sûr, en informatique classique, on peut faire du calcul en parallèle, en utilisant plusieurs processeurs ! Mais il existe une différence fondamentale entre les parallélismes quantique et classique. En effet, si on veut une augmentation exponentielle du calcul, en informatique classique, il faut une augmentation exponentielle de la taille (le nombre de processeurs); par contre, en informatique quantique, il suffirait d'une augmentation linéaire de la taille du système !

Avec l'algorithme de Shor, ne verrait-on pas apparaître des problèmes de sécurité, sachant que RSA est un des cryptosystèmes à clés publiques le plus utilisé ?

Effectivement, comme on sait que toute la sécurité de RSA est basé sur la factorisation d'un nombre entier, l'algorithme de Shor arriverait à casser RSA en quelques temps. En effet, si Alice désire envoyer des informations confidentielles à Bob, en utilisant RSA; avec l'algorithme de Shor, ses données ne resteraient plus confidentielles. Il suffirait à Ken d'utiliser cet algorithme pour factoriser le nombre en question, et ainsi avoir accès aux informations d'Alice. Cependant, la cryptographie quantique permettrait de résoudre ce genre de problème !