PC Quantique

- Informatique - Hardware -

Date de mise en ligne : mercredi 21 mars 2007

Spyworld Actu

L'ordinateur conventionnel ou classique commence à s'approcher lentement de ses limites. Avec l'actuelle technologie, les grandes firmes tels que Intel, AMD ou Motorola arrivent tant bien que mal, à concevoir des microprocesseurs ou « chips » dont les performances ne cessent de croître. Prenons comme exemple le dernier né des laboratoires Intel, le Core 2 Duo : Le Core 2 Duo 6300 dont la fréquence d'horloge est de l'ordre de 1,86 Ghz est de la taille de 111mm_ et intègre 167 millions de transistors ! Même chose avec un Pentium 4 avec ses 125 millions de transistors gravés sur une surface de 112mm_. Vous pouvez imaginer qu'avec de telles dimensions pour un si grand nombre de transistors, les problèmes de dissipation thermique et de gestion d'énergie sont loin d'être résolus quoique les ténors du monde des « puces intelligentes » nous livrent à chaque fois des chips plus performantes les unes que les autres, mais jusqu'à quand ?

De même il existe des problèmes, ou plutôt des calculs, que les ordinateurs actuels quelles que soient leurs puissances, sont tout simplement incapables de résoudre en des temps acceptables. Par exemple, dans les domaines de la cryptographie ou pour les applications qui nécessitent des calculs en parallèles et avec les algorithmes actuels il faut des milliers d'années pour le plus avancé des super calculateurs afin de réussir à délivrer un résultat. C'est le cas par exemple des codes d'encryption, impossible à casser même pour ceux ayant conçu le programme de cryptage et c'est ce qui explique d'ailleurs qu'ils sont largement utilisés par les services de sécurité de part le monde pour la protection de leurs données confidentielles.

C'est dans ce contexte que les recherches ont démarré au début des années 70 pour trouver, à long terme, des solutions à ces miniaturisations qui confèreront bientôt aux composants des dimensions atomiques et frôleront ainsi le domaine de la physique quantique. L'apparition du premier ordinateur quantique était attendue pour 2020 car il fallait trouver de nouveaux algorithmes et un nouveau moyen de programmation afin qu'ils délivrent le maximum de leurs performances. Mais il y'a une révolution dans tout ça, si nos PC utilisent des bits, les quantiques eux utilisent des qubits. Une petite explication s'impose : Un bit actuel ne peut présenter qu'un état parmi deux possibles soit 0 soit 1, un qubit ou plutôt le futur bit de l'informatique pourra aussi prendre la valeur de 0 ou de 1 mais aussi de 0 et de 1 en même temps ! Cette propriété lui confère ses capacités à effectuer des traitements en parallèle beaucoup plus rapidement que ceux qu'exécutent ses « ancêtres » actuels. Il peut ainsi casser une clé de cryptage en quelques secondes ou encore factoriser un nombre composé de 1000 chiffres en seulement 20 minutes, chose qui demande 10 millions de milliards d'années voire plus pour les ordinateurs de nos jours ! Mais pour tirer profit des capacités offertes par ce PC futuriste, il faut utiliser de nouveaux algorithmes, des algorithmes créés par des mathématiciens et des physiciens et qui ont donné pleine satisfaction. Les plus connus d'entre eux sont ceux de Shor qui permettent de factoriser de grands nombres (Mathématicien à l'MIT) et de Grover (Physicien aux laboratoires Bell) qui est utilisé en cryptographie mais aussi pour rechercher et trouver des enregistrements dans des bases de données non triées dans des temps remarquables.

Le mois dernier, à la surprise générale des chercheurs, une start-up canadienne du nom de D-Wave vient de dévoiler un prototype d'ordinateur quantique au nom d'Orion dont la commercialisation est annoncée pour l'an prochain. Son processeur a été conçu par D-Wave mais fabriqué par les ingénieurs de la NASA qui dispose de la technologie nécessaire pour le réaliser.

Ce dernier utilise des composants supraconducteurs qui fonctionnent en milieu cryogénique, très près du zéro absolu, et comporte 16 qubits. A un tel froid (- 273,15° C), les métaux peuvent se trouver dans les positions électriques 0 et 1 simultanément. D'autres techniques existent pour générer ces désormais fameux qubits mais présentent plusieurs inconvénients.

La piste de ces composants supraconducteurs est privilégiée car elle présente l'avantage de ne pas utiliser d'électricité pour générer une molécule dont les noyaux atomiques représentent les qubits.

Lors de la démonstration, Orion a réussi à résoudre un problème de sudoku, arrangé un plan de table par affinités de personnes et a pu vérifier une correspondance moléculaire en quelques minutes. La société propose de louer le temps de calcul d'Orion en attendant sa commercialisation, D-Wave compte aussi lancer une version à 32 qubits d'ici à la fin de l'année, puis des versions à 512 qubits et 1024 qubits en 2008 (un ordinateur quantique de 300 qbits pourrait gérer environ 10 puissance 90 informations, soit plus que le nombre d'atomes dans l'univers observable). Chose inimaginable diront, certains chercheurs et experts du domaine du quantique, car il faudrait résoudre le problème lié à l'azote et à l'hélium, ces deux liquides qui doivent être changés régulièrement du fait de leur évaporation, ces derniers sont indispensables au fonctionnement de l'ordinateur quantique en utilisant la méthode de D-Wave pour façonner les qubits, Ces mêmes qubits qui peuvent générer des calculs erronés si leur nombre devrait subir une hausse. La programmation aussi de ses machines pose problème, car jusqu'à l'instant il n'existe qu'un seul système que la société canadienne a testé et qui s'appelle Adiabatic Quantum Computation créé par un universitaire du MIT.

Et pour conclure, ces nouveaux ordinateurs qu'on n'est pas prêt à voir débarquer dans nos maisons avant quelques années vont certainement révolutionner le monde. A entendre parler ces créateurs, les mondes de l'informatique et de l'intelligence artificielle seront chambardés et les techniques qu'on utilise de nos jours pour sécuriser nos données et qu'on croyait jusqu'ici si infaillibles vont certainement cesser de fonctionner. La quantique a même gagné d'autres terrains, comme celui de la communication, un tel système existe et a même été testé par la British Telecom sur une ligne quantique sur une distance de 10km, cette innovation permet d'assurer la quasi confidentialité des appels passés, plus jamais ces appels ne pourront être mis sur écoute, et même si c'est le cas les interlocuteurs s'en apercevront facilement.

Que dire alors des constructeurs de disques durs, tel que Seagate, qui comptent axer leurs nouvelles stratégies sur la vente de disques intégralement chiffrés (Tout ce qui est écrit sur le disque dur est chiffré en direct, à la volée, sans que l'utilisateur ne se rende compte de rien. En sens inverse, la puce contenue dans ses disques déchiffre tout ce qui doit être lu).

Et si D-Wave réussit à commercialiser des ordinateurs quantiques d'ici 2008, les grosses boîtes de l'électronique vont certainement galérer car plus rien n'assurera la confidentialité des informations, et leurs produits n'auront aucune raison d'exister. Il faut aussi voir le bon côté des choses, peut-être qu'avec des lignes de communication quantiques, comme ceux testées actuellement par les opérateurs anglais, il n'y aura plus de problèmes de débits ni d'ADSL en général comme c'est malheureusement le cas chez nous !

Qui vivra verra...

Post-scriptum :

http://www.tunishebdo.com.tn/articl...