

UNIVERSITÉ DE LILLE

Groupe de travail multi-disciplinaire: Information quantique

Organisation: Stephan De Bièvre, A. Gomes, N. Melab, V. Vallet

INTRODUCTION. Un ordinateur exploitant subtilement les principes de base de la mécanique quantique pourra être spectaculairement plus efficace qu'un ordinateur classique, comme l'ont démontré théoriquement Shor (1994) et Grover (1996), en proposant des algorithmes quantiques capables de factoriser un très grand nombre premier très rapidement ou de repérer très rapidement une donnée dans une très grande liste non-organisée. Un protocole de partage de clé, appelé BB84 d'après ses inventeurs Bennett et Brassard (1984), exploitant astucieusement l'existence d'observables incompatibles et le principe d'incertitude peut assurer une sécurité cryptographique inégalée. Ces résultats et quelques autres ont donné lieu à une nouvelle science, à la jonction de l'informatique, de la théorie de l'information et de la mécanique quantique: l'information quantique, qui englobe notamment la cryptographie quantique et le calcul quantique. Ses promesses, non totalement tenues pour l'instant, et issues de quarante ans de recherches scientifiques interdisciplinaires, attirent aujourd'hui, partout dans le monde, les investisseurs privés comme publiques vers la technologie quantique.

GROUPE DE TRAVAIL. Le but de ce groupe de travail est de réunir l'ensemble des acteurs de l'Université de Lille intéressés par ce sujet. Le groupe de travail se réunira dans un premier temps tous les six semaines, a priori un vendredi après-midi. À chaque fois, il y aura deux exposés de 40 minutes chacun, suivi d'une session de questions et de discussion de 15 minutes. Les exposés seront destinés à un large public interdisciplinaire de chercheurs et d'enseignant-chercheurs, qu'ils soient étudiants, doctorants, postdoctorants ou plus expérimentés, afin de permettre à chacun de se familiariser avec divers aspects de l'information quantique. Des séances plus spécialisées seront organisées ultérieurement ou en parallèle, selon les intérêts des participants.