Cryptographie quantique avec des appareils malicieux

Frédéric Dupuis*[1]

[1]CNRS, LORIA – - – France

Résumé

La mécanique quantique nous permet d'accomplir certaines tâches cryptographiques qui sont impossibles classiquement, comme par exemple générer une clé secrète entre deux participants seulement à l'aide d'un canal public. Or, ces protocoles quantiques supposent que les participants ont accès à des appareils qui fonctionnent exactement selon les spécifications. En pratique, une telle perfection est malheureusement difficile à atteindre. Pire: l'appareil pourrait même être fourni par un manufacturier malicieux tentant de briser le protocole pour son propre compte. Pour mitiger ce problème, des protocoles dont la sûreté peut être vérifiée seulement à partir du comportement observable des appareils ont été développés. La sûreté de ces protocoles dits "device independent" est cependant beaucoup plus difficile à démontrer. Dans cet exposé, je présenterai une nouvelle méthode permettant de borner la quantité d'aléa généré par un processus quantique à n étapes, et qui mène à des bornes de sécurité optimales pour plusieurs protocoles cryptographiques. Travail conjoint avec Rotem Arnon-Friedman, Omar Fawzi, Renato Renner et Thomas Vidick

*Intervenant