Computational assumptions in quantum cryptography

Paul Dumais
Département d'informatique et de recherches opérationnelles
Université de Montréal
C.P. 6128, Succ. Centre-ville
Montréal, Québec
CANADA H3C 3J7

Abstract

Outre la communication secrète, la cryptographie moderne s'intéresse aux protocoles permettant à deux parties qui ne se font pas confiance d'effectuer un calcul commun sur des données secrètes à chacune. Afin d'établir la sécurité d'un protocole, on doit généralement faire la démonstration que tout comportement dangereux de la part d'une des parties est théoriquement équivalent à l'accomplissement d'une tâche considérée infaisable. La plupart des protocoles en usage aujourd'hui sont basés sur l'hypothèse qu'il est infaisable de factoriser de grands nombres entiers. L'avènement de l'ordinateur quantique pourrait bouleverser ces idées reçues car un algorithme quantique pour factoriser des grands nombres existe déjà sur papier. De plus, un théorème d'impossibilité interdit tout espoir d'implanter avec sécurité inconditionnelle, même dans le modèle quantique, la "mise en gage de bit", une primitive cryptographique fondamentale. La cryptographie bipartite vit désormais sous la menace d'un hypothétique ordinateur quantique.

Nous nous intéressons donc aux conséquences théoriques sur la cryptographie de la prise en compte du paradigme du calcul quantique, en particulier à la possibilité de fonder les primitives de "mise en gage de bit" et de "transfert inconscient" sur des hypothèses calculatoires quantiques. Nous montrons que ces deux primitives peuvent

être construites sous l'hypothèse que des "permutations à sens unique" quantiques existent.

The "bit commitment" primitive is a key ingredient in two party cryptography where both participants want to compute a public function of their private inputs. Since the discovery of the impossibility theorem stating that unconditionally secure quantum bit commitment cannot exists, quantum cryptography in the two party case must rely on assumptions. We are considering quantum computational assumptions. Those assumptions have to be different from their classical cousins since "factoring large integers", a computational assumption widely in use nowadays, is under attack by a quantum algorithm.

We are interested in the possibility of basing the "bit commitment" and "oblivious transfer" cryptographic primitives on quantum computational assumptions. We show that those two primitives can be constructed if we assume that quantum "one-way permutations" exist.