Université de Limoges **Année universitaire 2016-2017**
Faculté des Sciences et Techniques

PIR : La sécurité contre les attaques quantiques

PHAN Duong Hieu

Résumé. La mise en œuvre éventuelle de machines quantiques rendrait plusieurs schémas cryptographiques vulnérables. En effet, de nombreux problèmes peuvent être résolus en temps polynomial par des machines quantiques comme la factorisation et le logarithme discret (qui font partie d'une classe de problèmes dits de sous- groupe caché dans des groupes abéliens) qui sont largement utilisés dans des systèmes pratiques. Il est par conséquent utile d'étudier des constructions basées sur des problèmes algorithmiques qui sont considérés difficiles à résoudre par des machines quantiques. Les problèmes algorithmiques demeurant non résolus par les machines quantiques sont à titre d'exemple : décodage des codes linéaires ; la recherche du vecteur le plus court dans un réseau (lattice); le problème de sous-groupe caché dans des groupes non abéliens (l'isomorphisme de graphes par exemple), etc. Des constructions de schémas cryptographiques ayant comme base ces problèmes sont envisageables. Dans notre projet de stage, nous nous intéressons aux problèmes de la théorie des codes et aux problèmes de réseaux.

Référence.

- A Decade of Lattice Cryptography
`https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf`
- Hardness of k-LWE and Applications in Traitor Tracing `http://www.di.ens.fr/users/phan/2016_LBTTlong.pdf`