

Titre et Mise en Cohérence des Objectifs du TIPE

Élie Besnard, Malo Leroy, Yun Marcola

Ancrage au thème : L'augmentation de la connectivité dans les zones urbaines et de la puissance de calcul à disposition entraîne le besoin de développer des transmissions de données toujours plus sécurisées.

(28 mots)

Motivation : Nous avons choisi ce sujet afin de nous pencher sur la vaste théorie de la Mécanique Quantique afin d'en découvrir certains principes et d'en appréhender une application concrète.

Mots-Clés :

- Informatique / Computer Science
- Cryptographie / Cryptography
- Mécanique Quantique / Quantum Mechanics
- Algèbre Linéaire / Linear Algebra
- Arithmétique / Arithmetic

Positionnement Thématique :

- Informatique (Cryptographie)
- Physique (Mécanique)
- Mathématiques (Algèbre Linéaire)

Bibliographie :

1. Claude Cohen-Tanoudji, Bernard Diu et Franck Laloë. *Mécanique Quantique*. éditions Hermann, ISBN : 978-2-7598-2287-4
2. Richard Feynman. *Le cours de physique de Feynman*, tome 5, éditions Dunod, ISBN : 978-2-1000-4934-8
3. *Algorithme de Shor*, Wikipédia, https://fr.wikipedia.org/wiki/Algorithme_de_Shor

Bibliographie Commentée : En premier lieu, nous nous sommes intéressés au fondement de la Cryptographie Quantique : l'algorithme de Shor (3). Cet algorithme conçu pour être exécuté sur un ordinateur quantique permet de factoriser un entier en produit de facteurs premiers avec une remarquable efficacité. Mais pour pouvoir approfondir nos recherches sur le sujet, nous avons dû nous familiariser avec les bases du formalisme de la mécanique quantique et de son cadre mathématique. Nous avons pour cela parcouru différents ouvrages (1) et (2) de grandes figures de la Physique Quantique.

Problématique : Comment la Mécanique Quantique pourrait nous permettre de sécuriser nos échanges de données pour les années à venir ?