

Master Informatique

Informatique et calcul quantique

Responsables	Descriptions	Informations
Giuseppe DI MOLFETTA giuseppe.DI-MOLFETTA@univ-amu.fr	Code : S51IN2M04	Composante : Faculté des Sciences
Pablo ARRIGHI pablo.ARRIGHI@univ-amu.fr	Nature : Unité d'enseignement Domaines : Sciences et Technologies	

CONTENU

Cette unité d'enseignement a pour vocation de faire découvrir aux étudiants les spécificités et les possibilités qu'ouvrent le traitement quantique de l'information et de leur donner les bases pour décrire et analyser des circuits quantiques simples.

On montrera comment la mise au point d'algorithmes quantiques permet de résoudre certains problèmes de façon exponentiellement plus efficace que les algorithmes classiques traditionnels (recherche, tri, ...), et notamment le problème de la factorisation des grands nombres. Il s'en suit que la mise au point d'un ordinateur quantique de grande taille remettrait en cause les algorithmes à clés publiques aujourd'hui utilisés pour sécuriser Internet (d'où la nécessité d'une post-quantum cryptography).

On introduira également les idées principales du domaine de la cryptographie quantique. On évoquera les possibilités offertes par ce nouveau paradigme dans d'autres champs de l'informatique, tels que le machine learning.

Contenu :

1. Fondamentaux du calcul quantique I (linéarité de la théorie, qubits, superpositions, intrication);
2. Fondamentaux du calcul quantique II (portes quantiques et circuits)
3. Algorithme quantique de Grover; (iii) Algorithme de Shor et Cryptage RSA;
4. Éléments de cryptographie quantique.

PRÉREQUIS RECOMMANDÉS

Bases d'algèbre linéaire (L1), Algorithmique (Licence Info), Complexité (M1 Informatique).

VOLUME HORAIRE

- Volume total: 27 heures

CODES APOGÉE

- SINBU08L [ELP]

POUR PLUS D'INFORMATIONS

[Aller sur le site de l'offre de formation...](#)



Dernière modification le 23/06/2022