Module : Cryptographie quantique				Code	
				ING-4-SSIR-S8-P2	
Période	**Semestre 1**	*Volume horaire*	**21 H**	*ECTS*	**2**

Responsable	Iyed ben slimen	*email*	iyed.enicar@gmail.com
Equipe pédagogique	Iyed ben slimen		

1. Objectifs de Module *(Savoirs, aptitudes et compétences)*

Ce module porte sur l'informatique et les communications quantiques et leurs applications afin de distribuer les clés d'un crypto système symétrique.

Acquis d'apprentissage :

A la fin de cet enseignement, l'élève sera capable de :

Compétences
C2.1 -Maîtriser les notions de qubits et registres à deux qubits. -Maitriser les phases des protocoles BB84 avec codage de polarisation et codage de phase, le protocole Six State, le protocole B92, et le protocole EPR.
C1.2 -Caractériser les portes quantiques et les mesures à un ou deux qubits -Décrire le transport des photons individuels et intriqués, ainsi que les défis matériels
C1.3 Simuler et tester des portes quantiques et mesures avec téléportation quantique
C3.3 Se sensibiliser de l'importance de migration vers de solutions « quantum safe » soient PQC ou QKD

2. Pré-requis*(autres UE et compétences indispensables pour suivre l'UE concernée)*

- Circuits logiques
- Algorithmique
- Connaissances élémentaires en optique
- Mathématiques des espaces vectoriels

3. Répartition d'Horaire de Module					
Intitulé de l'élément d'enseignement	***Total***	***Cours***	***TD***	***Atelier***	***PR***
Module : **Cryptographie quantique**	21H	10.5H	9H	1.5H	

4. Méthodes pédagogiques et moyens spécifiques au Module
(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Supports de Cours
- Projecteur et Tableau
- Travaux dirigés
- Logiciels de simulation : Accès à la plateforme IBM Quantum

Bibliographie

Titre	**Auteur(s)**	**Edition**
Technologies quantiques vers la seconde révolution	Michle Kurek	Ecole polytechnique de Paris, 2021
Qunatum Information Science for Computer Scientists	Gilles Brassard	Université Montréal, 2017
Learn Quantum Computing with python and IBM quantum Experience	Robert Lerodo	Packt Publishing Ltd. Birmingham, 2020
Introduction à l'information quantique	Y. Leroyer et G. Sénizergues	ENSEIRB-MATMECA, 2017
Contribution à l'étude et à la réalisation d'un système de distribution quantique de clef par codage en phase	Séabastien Agnolini	HAL Id: pastel-00003416 Année : 2008

5. Contenu	Durée allouée	
Module 1 : Qubits.		
Séance 1 • Introduction à l'informatique quantique • Exemples de réalisation des qubits • Découverte de la plateforme de l'IBM	Cours Atelier	2.5H 0.5H
Séance 2 • Mesures sur un qubit • Transformations d'un qubit • Exercices TD • TP de transformations et mesures sur IBM QUANTUM	Cours Atelier	2.5H 0.5 H

Module 2 : Protocoles de QKD		
Séances 4, 5 et 6 • Cryptographie classique et cryptographie quantique : défis et technologies • PQC versus QKD • Protocole BB84 avec codage de polarisation • Protocole BB84 avec codage de phase • Attaque Intercept and Resend • Attaque de duplication • Attaque Beam Splitting • Protocole Six State • Protocole B92 • Exercices TD	Cours	9H
Module 3 : Intrication quantique		
Séances 6 et 7 • Registre quantique à deux qubits • Etats intriqués • Mesures sur les états intriqués • TP de téléportation sur IBM quantum • Protocole EPR	Cours Atelier	5.5 H 0.5 H

6. Mode d'évaluation de Module*(nombre, types et pondération des contrôles)*

Eléments d'enseignement	Coeff	DS	EX	TP	PR
Module – Cryptographie quantique	1	30%	60%	10%	

Pour valider le module, les étudiants passeront un examen dont le coefficient est de 60%, un DS dont le coefficient est de 30% et un TP dont le coefficient est de 10%.

La durée de tous les examens (Examen, DS…) est de 1h30.

Le DS est planifié 4 semaines après le début du module.
Quant à l'examen, il est planifié après l'écoulement des 7 semaines et portera sur toutes les thématiques enseignées tout au long des 21 heures.

Concernant le TP, il est planifié une semaine avant l'examen et testera les connaissances acquises tout au long du module.

Le module est validé si l'étudiant obtient une moyenne supérieure ou égal à 10 sur 20.