Journal de bord du module
Cryptographie quantique
Les renvois de la table de matières sont cliquables.

Table des matières

1 Notes du cours et recueil des exercices des travaux dirigés

Notes de cours: version préliminaire. Une version avec quelques corrections sera mise en ligne la première semaine de mars 2020.

Recueil des exercices des travaux dirigés

2 Correction de l'examen du 18 février 2020.

Correction de l'examen du 12 décembre 2018.

3 Introduction et motivation

— Brève histoire des sciences.
— Historique du développement informatique de 1946 à nos jours.
— Perspectives de l'évolution technologique.
— Diaporama de la première séance. ← Fin du cours du 07 janvier 2020.

4 Rappels sur la théorie des probabilités

— Description d'une expérience physique en termes d'un modèle statistique.
— Espace probabilisé.
— Variables aléatoires.
— Représentation des variables aléatoires en termes de noyaux stochastiques.
— Noyaux stochastiques déterministes associés à des variables aléatoires.
— Loi d'une variable aléatoire comme action gauche du noyau stochastique associé sur la probabilité de départ.
— Résolution projective de l'identité. Probabilités à valeurs fonctions indicatrices.
— Effets francs classiques et observables franches classiques.
— Effets classiques flous. Résolution positive de l'identité. ← Fin du cours du 17 janvier 2020.

5 Postulats de le mécanique classique (vue comme une théorie des probabilités munie d'une règle dynamique)

— Énoncé des postulats.
— Illustration des postulats sur un exemple discret.
— Les postulats classiques ne permettent pas de décrire la Nature.
— Inégalités de Bell, expérience d'Orsay et réfutation de l'hypothèse de variables cachées.

6 Postulats de le mécanique quantique (dans un cadre hilbertien simplifié)

Les postulats sont présentés dans le même ordre que les postulats de la mécanique classique pour pouvoir faire le parallèle immédiat.

- Énoncé des postulats.
- Illustration des postulats sur un exemple en dimension 2 (qubit). ← Fin du cours du 21 janvier 2020.

7 Quelques notions importantes sur les espaces de Hilbert

- Théorème spectral pour les opérateurs normaux (en dimension finie).
- Produit tensoriel d'espaces vectoriels. Définition et construction. Bases dans l'espace produit tensoriel.
  - Produit scalaire sur le produit tensoriel de deux espaces de Hilbert.
  - Quelques précisions et exemples sur le produit tensoriel.
  - Produit tensoriel d'opérateurs.
  - Tenseurs simples et tenseurs intriqués. Signification en classique et en quantique. ← Fin du cours du 23 janvier 2020.
- Notation de Dirac.
- Opérateurs positifs. classe trace. Norme de la trace. Opérateur densité.
- Formulation complète du postulat des états.
- Trace partielle. ← Fin du cours du 24 janvier 2020 (matin).
- Marginales quantiques. ← Fin du cours du 24 janvier 2020 (après-midi).
- TD du 24 janvier 2020 (après-midi): Exercices 1-2c.

8 Premières conséquences du formalisme quantique

- Précisions sur le calcul des traces partielles et marginales quantiques. Les marginales d'un état pur du système composé peuvent être maximalement mélangées.
- Relation d'incertitude de Heisenberg.
- Paradoxe d'Einstein, Podolsky et Rosen (début).← Fin du cours du 28 janvier 2020 (première séance.

9 Distribution de la clé par un procédé quantique

- Rappel sur le chiffrement de Vernam offrant une sécurité inconditionnelle (informationnelle).
- Théorème de non-clonage des états quantiques non-orthogonaux et non-collinéaires.
- Protocole BB84 de distribution quantique de la clé.
  - Génération de la clé du côté d'Alice.
  - Génération de la clé du côté de Bernard.
  - Algorithme de conciliation.
  - Comportement asymptotique du nombre de coïncidences dans le cas de non-intrusion.
  - Détection de l'intrusion éventuelle et réconciliation. ← Fin du cours du 28 janvier 2020 (2e séance).

— TD du 29 janvier 2020: Exercices 2d–9.2.

10 Analyse de la sécurité du protocole BB84 pour des intrusions plus subtiles

— Effets flous (classiques et quantiques).
— Établissement d'une borne grossière du gain informationnel de l'intrus par rapport en fonction de la distortion sur les bits du récipiendaire.
— Amélioration de la borne précédente : $I(\mathbf{p} : \mathbf{q}) \leq \frac{1}{2}\phi(\mathbb{E}D)$, où $I(\mathbf{p} : \mathbf{q})$ représente l'information mutuelle entre les lois de génération de la clé de l'expéditeur et de l'intrus, D la distortion sur les bits de récipiendaire et ϕ une fonction explicitement connue. ← Fin du cours du 04 février 2020.
— TD du 04 février 2020: Exercices 9.3–9.4, 11–12, 14–15.
— TD du 05 février 2020: Exercices 16, 18–24.1.

11 Registres et portes logiques

— Registres classiques.
— Enregistrer un bit d'information coûte de l'énergie ; effacer un bit d'information produit de l'énergie qu'il faut dissiper.
— Principe de Landauer : apprendre en fin de calcul la valeur prise par un bit, cause l'augmentation de l'entropie d'au moins $1.38 \times \ln 2 \times 10^{-23}$ J/s quelque part dans l'univers.
— Registres quantiques.
— Portes logiques classiques et fonctions booléennes.
— Portes logiques quantiques unitaires.
— Approximation d'un opérateur unitaire.
— Portes de Hadamrd, contrôlées et multi-contrôlées, de phase. ← Fin du cours du 07 février 2020.

12 Algorithmes quantiques

12.1 Algorithme de Deutsch-Josza

— Fonctions booléennes constantes, fonctions booléenes équilibrées.
— Accélération exponentielle pour déterminer si une fonctions booléenne est constante ou équilibrée. ← Fin du cours du 11 février 2020.
— TD du 11 février 2020: Exercices 24.2–27.

12.2 Algorithme de Shor

— Transformée de Fourier quantique son implémentation par un circuit quantique.
— Problème d'estimation de la phase.

— Circuit quantique pour l'estimation de la phase et calcul de la probabilité d'erreur pour une précision de l'estimation) n bits.
— Exponentiation modulaire et définition de l'ordre.
— Algorithme classique du développement en fraction continue.
— Algorithme et circuit quantique de détermination de l'ordre.
— Algorithme de factorisation de Shor.

13 Authentification

Quelques notions et présentation d'un algorithme quantique d'authentification sans intrication. ← Fin du cours du 18 férvrier 2020 et fin du module.