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

Table des matières

1 Correction de l'examen du 12 décembre 2018.

Correction de l'examen du 12 décembre 2018.

2 Notes du cours et recueil des exercices des travaux dirigés

Notes de cours: version préliminaire

Recueil des exercices des travaux dirigés

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 4 octobre 2018.

4 Rappels sur la théorie des probabilités

— Description d'une expérience physique en termes d'un modèle statistique.
— Espace probabilisé.
— Variables aléatoires.
— Complexité de Kolmogorov.
— Réductibilité de l'aléa classique.
— Il n'existe pas d'algorithme classique ou de dispositif physique classique fini permettant de générer une suite de variables aléatoires (classiques).
— 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. ← Fin du cours du 9 octobre 2018.
— Effets classiques flous. Résolution positive de l'identité.

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.
— L'expérience d'Orsay comme jeu impossible à gagner, quelle que soit la stratégie déterministe ou aléatoire utilisée. ← Fin du cours du 11 octobre 2018.

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 06 novembre 2018.
— TD du 07 novembre 2018: Exercice 2.

7 Quelques rappels sur les espaces de Hilbert

— Espaces vectoriels à produit scalaire, norme hilbertienne, espace de Hilbert.
— Produit scalaire hermitien, inégalité de Buniakovski-Cauchy-Schwarz, norme hilbertienne.
— Formes linéaires, dualité. Dual algébrique. ← Fin du cours du 07 novembre 2018.
— TD du 08 novembre 2018: Exercices 1, 3–5, 6 (preuve de l'unicité ; l'existence sera établie à la prochaine séance.
— Dual topologique.
— Opérateurs linéaires, norme opératorielle.
— Opérateur adjoint.
— Opérateurs normaux, auto-adjoints, anti-afdjoints, unitaires.
— Projections, orthoprojections, orthoprojections orthogonales.
— 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. ← Fin du cours du 13 novembre 2018.
— Quelques précisions et exemples sur le produit tensoriel.
— Produit tensoriel d'opérateurs.
— Notation de Dirac.
— Opérateurs positifs. ← Fin du cours du 14 novembre 2018.
— Norme de Hilbert-Schmidt.
— Trace pour les opérateurs de classe trace. Norme de la trace. Opérateur densité.
— Formulation complète du postulat des états.
— Trace partielle. Marginales quantiques.

8 Premières conséquences du formalisme quantique

— Précisions sur le calcul des traces partielles et marginales quantiques. (Début). ← Fin du cours du 15 novembre 2018.
— Fin du calcul : les marginales d'un état pur du système composé peuvent être maximalement mélangées.
— Relation d'incertitude de Heisenberg.
— Les polariseurs ne sont pas des filtres classiques. ← Fin du cours du 16 novembre 2018.
— Décomposition de Schmidt d'un vecteur dans le produit tensoriel.
— Opérateurs densité classiquement corrélés, opérateurs non-classiquement corrélés.

— Intrication.
— Paradoxe d'Einstein, Podolsky et Rosen (début). ← Fin du cours du 20 octobre 2018.
— Paradoxe d'Einstein, Podolsky et Rosen (fin). ← Fin du cours du 21 novembre 2018.
— TD du 21 novembre 2018: Exercices 13, 21.
— TD du 22 novembre 2018: Exercices 23, 24.

9 Distribution de la clé par un procédé quantique

— Rappel sur le chiffrement de Vernam. ← Fin du cours du 22 novembre 2018.
— 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 novembre 2018.

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 : $I(\pi : p) \leq \frac{1}{2}\phi(\mathbb{E}D)$, où $I(\pi : p)$ 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 29 novembre 2018.

11 Éléments de calcul quantique et factorisation de Shor

Ce chapitre ne sera pas examiné à l'examen final.

— Portes classiques pour fonctions booléennes.
— Portes classiques réversibles.
— Portes quantiques.
— Porte de Hadamard, portes de phase, portes contrôlées et multicontrôlées.
— Algorithme de Shor.
  — Transformée de Fourier discrète ; transformée de Fourier quantique.
  — Estimation de la phase.
  — Problème de détermination de l'ordre.
  — Factorisation. ← Fin du cours du 30 novembre 2018 et fin du programme.
— Diaporama du cours du 30 novembre 2018.