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

Table des matières

4 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 20 septembre 2017, après-midi.

5 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 27 septembre 2017.

6 Quelques rappels sur les espaces de Hilbert

— Espaces vectoriels à produit scalaire, norme hilbertienne, espace de Hilbert. ← Fin du cours du 28 septembre 2017.
— TD du 28 septembre 2017: exercices 1–2.
— Produit scalaire hermitien, inégalité de Buniakovski-Cauchy-Schwarz, norme hilbertienne.
— Formes linéaires, dualité. Dual algébrique, dual topologique.
— Opérateurs linéaires, norme opératorielle. FinCours4 octobre 2017.
— TD du 4 octobre 2017: exercices 3–5.
— 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. ← Fin du cours du 10 octobre 2017.
— Produit scalaire sur le produit tensoriel de deux espaces de Hilbert.
— Produit tensoriel d'opérateurs.
— Notation de Dirac.
— Opérateurs positifs.
— Trace pour les opérateurs de classe trace. Opérateur densité.
— Formulation complète du postulat des états.
— Trace partielle. Marginales quantiques. ← Fin du cours du 11 octobre 2017.
— TD du 11 octobre 2017: exercices 9–13.

7 Premières conséquences du formalisme quantique

— Relation d'incertitude de Heisenberg.
— Les polariseurs ne sont pas des filtres classiques.
— Précisions sur le calcul des traces partielles et marginales quantiques.
— Décomposition de Schmidt d'un vecteur dans le produit tensoriel.
— Opérateurs densité classiquement corrélés, opérateurs non-classiquement corrélés.
— Intrication. ← Fin du cours du 16 octobre 2017.
— TD du 17 octobre 2017: exercices 21 et 23.
— Paradoxe EPR (Einstein-Podolsky-Rosen).

8 Distribution de la clé par un procédé quantique

— Chiffrement de Vernam ; théorème de Shannon sur le chiffrement de Vernam.
— Théorème de non-clonage des états quantiques non-orthogonaux et non-collinéaires. ← Fin du cours du 17 octobre 2017.
— 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.

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

— Effets flous (classiques et quantiques). ← Fin du cours du 24 octobre 2017.
— 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 25 octobre 2017.
— TD du 25 octobre 2017: exercice 20 : 1–4.
— Contrôle continu du 14 novembre 2017, 8h–9h. La solution est consultable ici.

10 Éléments de calcul quantique et factorisation de Shor

— Portes classiques pour fonctions booléennes.
— Portes classiques réversibles.
— Portes quantiques.
— Réalisation des opérateurs unitaires.

— Porte de Hadamard, portes de phase, portes contrôlées et multicontrôlées. ← Fin du cours du 14 novembre 2017.