

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

Table des matières

1	Introduction et motivation	1
2	Introduction à la mécanique quantique	2
3	Rappels des propriétés élémentaires des espaces de Hilbert utiles en information quantique	2
4	Cryptographie	2
5	Espaces de Hilbert et opérateurs (suite)	2
6	Rappels sur l'entropie	2
7	Analyse de la sécurité du protocole BB84	3
8	Machines de Turing, classes de complexité	3
9	Principes du calcul quantique	3
10	Algorithme de factorisation de Shor	3
11	Lien utiles	3

1 Introduction et motivation

- Historique du développement informatique de 1946 à nos jours.
- Perspectives de l'évolution technologique.
- [Transparents du développement historique](#)

2 Introduction à la mécanique quantique

- Un bref aperçu de la physique classique comme une théorie des probabilités ; postulats d'un système classique.
- Version de von Neumann des postulats de la mécanique quantique.

3 Rappels des propriétés élémentaires des espaces de Hilbert utiles en information quantique

- Produit scalaire, norme.
- Opérateur adjoint, norme d'un opérateur, opérateurs bornés.
- Opérateurs auto-adjoints, opérateurs unitaires.
- Produit tensoriel de deux espaces vectoriels, produit tensoriel d'opérateurs.

4 Cryptographie

- Code de Vernam.
- Théorème de non-clonage.
- Protocole BB84 de distribution d'une clé quantique :
 - Génération de la clé (coté Alice) ;
 - Génération de la clé (coté Bob) ;
 - Réconciliation ;
 - Détection d'une éventuelle intrusion ;
 - Distribution de la clé.
 - Détection de l'intrusion.

5 Espaces de Hilbert et opérateurs (suite)

- Théorème spectral.
- Opérateurs positifs, matrices densité.
- Résolutions de l'identité.
- Résolution projective (PVM) et résolution non-projective (POVM).

6 Rappels sur l'entropie

- Définition et trois interprétations différentes de l'entropie.
- Entropie conjointe, entropie conditionnelle.
- Information mutuelle.

7 Analyse de la sécurité du protocole BB84

- Gain moyen sur la prédiction des bits envoyés par Alice en termes d'une mesure non-projective effectuée par Ève.
- Perturbation moyenne sur les mesures projectives de Bernard due à l'intrusion d'Ève.
- Borne semi-cyclique.
- Borne de l'information mutuelle.

8 Machines de Turing, classes de complexité

- Machine de Turing déterministe ; classes de complexité P et PSPACE.
- Machine de Turing non-déterministe ; classe de complexité NP.
- Machine de Turing probabiliste ; classe de complexité BPP.
- Circuits booléens.
- Information classique, entropie, réversibilité.
- Systèmes composés, produit tensoriel, enchevêtrement.
- Portes logiques réversibles ; universalité de la porte de Fredkin.
- Machine de Turing pré-quantique ; machine de Turing quantique ; classe de complexité BQP.
- **Un exposé de vulgarisation sur l'irréversibilité, l'entropie et la production d'information.**

9 Principes du calcul quantique

- Portes réversibles classiques, portes de permutation.
- Portes quantiques.
- Réalisation approchée d'opérateurs unitaires.
- Portes de Hadamard, de phase, NOT contrôlée et bi-contrôlée, additionneur quantique.

10 Algorithme de factorisation de Shor

Version manuscrite de l'algorithme.

11 Lien utiles

Recueil d'exercices pour ce cours

État de lieu (en 2000) des algorithmes classiques de factorisation

Expérience de distribution quantique de la clé dans l'atmosphère

La cryptographie quantique devient une réalité industrielle