

Le Groupement National De Recherches - Information Quantique (GNDR-IQ)

en collaboration avec

La Faculté des Sciences-Rabat et Le LPHE-Modelisation & Simulation-FSR
organisent une

Ecole Nationale (Seconde édition)

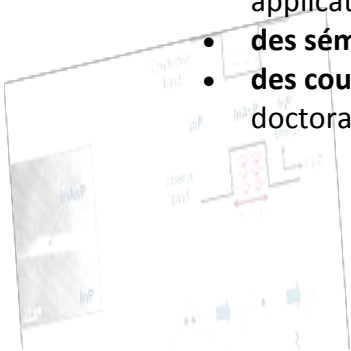
Théorie Quantique de L'Information: Fondements et applications **31 Janvier et 01 Février 2014**

La convergence de la théorie de l'information classique et de la physique quantique a ouvert des perspectives de recherches très prometteuses pour coder et transmettre de l'information en exploitant les propriétés étranges du monde quantique. Aussi, l'information quantique est un domaine récent des Sciences et Technologies de l'Information et de la Communication (STIC) qui est en plein développement. Des grands centres de recherches publics et privés ont été créés, ces dernières années, pour étudier et manipuler des systèmes quantiques à des fins de traitement de l'information. Bien que cela puisse sembler à caractère purement fondamental, les scientifiques sont fermement convaincus qu'il pourrait mener à des applications technologiques révolutionnaires. Les travaux accomplis jusqu'à maintenant mettent en avant des capacités inédites de protocoles et algorithmes quantiques à résoudre efficacement certains problèmes mathématiques réputés difficiles. L'engouement pour cette nouvelle thématique s'explique aussi en grande partie par la découverte de protocoles quantiques inconditionnellement sûrs d'échanges de clefs cryptographiques (cryptographie quantique). Les progrès considérables de la nano physique, qui permettent la réalisation de la cryptographie quantique, laissent envisager un futur possible pour l'ordinateur quantique.

Le but principal de la seconde édition de cette école marocaine, organisée conjointement par **Le Groupement National De Recherches - Information Quantique, le Laboratoire de Physique des Hautes Energies Modélisation et Simulation** et **la Faculté des Sciences de Rabat**, est de permettre à l'ensemble des chercheurs travaillant en Information Quantique de se retrouver pendant 2 jours, afin d'échanger et de communiquer sur les dernières avancées du domaine.

L'école est organisée selon 3 modes de communications :

- **des conférences**, à caractère pédagogique soutenu, sur les fondements et les applications les plus avancées du domaine ;
- **des séminaires** sur les sujets d'actualité et d'applications de l'information quantique;
- **des courtes présentations de 15 mn** afin de permettre aux jeunes chercheurs et doctorants de présenter leurs résultats à l'ensemble de la communauté.





Faculte des Sciences, Universités Mohamed V- Agdal
Et

Groupeement National De Recherches - Information Quantique
en collaboration avec

Le LPHE-Modelisation & Simulation-FSR

• *organisent une*

Ecole Nationale (2eme édition)

Théorie Quantique de L'Information:

Concepts & Applications

Thèmes

Information Quantique

Sécurité Quantique

Corrélations Quantiques

Protocoles de Calculs Quantiques

Cryptographie Quantique

Circuits Quantiques



31 Janvier et 01 Février 2014

Fac Sciences-Rabat

Comité d'Organisation R. Ahl Laamara (LPHE-MS, Fac Sciences, Rabat), A. Azhari (Univ Hassan II, Casablanca), M. Bennai (Univ Hassan II, Casablanca), M. Daoud (Fac Sciences, Agadir), L.B. Drissi (Fac Sciences, Rabat), NE Fahssi (Univ Hassan II, Casablanca), E.H Saidi (Fac Sciences, Rabat)

PROGRAMME

Vendredi 31 Janvier 2014: Matinée (Amphi A, ENSET-Rabat)

08h30-09h00 : Ouverture de l'Ecole

Directeur de L'ENSET de Rabat

Directeur du Centre de Physique Mathématique

Coordinateur du Groupement National de Recherche -Information Quantique-

Président de l'Association Marocaine de Cryptographie

Chairman E.H Saidi (Univ Mohamed V-Agdal)

09h00-09h40: Introduction aux mystères de la physique et la cryptographie quantiques

H. Zbinden, Université de Genève - Suisse

09h40-10h20 : Schéma unificateur des corrélations en théorie quantique de l'information

M. Daoud, FS, Université Ibn Zohr, Agadir

10h20-10h35 : Pause-café

Chairman A. Azhari (Univ Hassan II, Casablanca)

10h35-11h15: L'Effet de la dépolarisation sur QKD

H. Ez-Zahraouy, FS, Université Mohamed V-Agdal

11h15-11h55: Post quantum cryptography based on SVP

A. Nitaj, Université Caen, France

11h55-12h35: Sur la séparabilité des états mixtes Quantiques

N. Boudi, Université My Ismail, Meknès

Vendredi 31 Janvier 2014 : Après midi (Amphi A, ENSET-Rabat)

Chairman N. Boudi (Univ My Ismail, Meknès)

14h30-15h00 : Implémentation de l'Algorithme de Grover en Cavité QED

M. Bennai, Université Hassan II Casablanca

15h00-15h30: Cryptographie Quantique avec des Etats Cohérents

M. Daoud, FS, Université Ibn Zohr, Agadir

15h30-16h00 : Garbling Circuits

H. Ben-azza, Université My Ismail, ENSAM, Meknès

16h00-16h30 : Réunion du Comité du GDRN-IQ

16h00-16h30 : Pause-Café &

Chairman M. Daoud (Univ Ibn Zohr, Agadir)

16h30-17h00 : Cryptographie chaotique et exemples de cryptosystèmes à clé publique

A. Azhari, Université Hassan II, Casablanca

17h00-17h20 : Autour de la Discorde Quantique

R. Essaber, R. Ahl Laamara, M. Daoud, LPHE-FS, Université Mohamed V-Agdal-Rabat

17h20-17h40 : Implémentation des protocoles Quantiques en Cavité QED

S. Taoufig, M. Bennai, Université Hassan II Mohammedia

17h40-18h00 : Corrélations dans des Etats Gaussiens

W. Kaydi, R. Ahl Laamara, M. Daoud, LPHE-FS, Université Mohamed V-Agdal-Rabat

18h00-18h30 : Discussion

Samedi 1 Février 2014 : Matinée (Amphi-Ibn Al Haytham, Fac Sciences, Rabat)

Chairman A. Nitaj (Univ Caen, France)

09h00-09h40 : Possibilités et limites des distributions de clés quantiques

H. Zbinden, Université de Genève - Suisse

09h40-10h10 : Codes Correcteurs et Algèbre de Lie

N. Fahssi, FST, Université Hassan II, Mohammedia

10h10-10h40: IBE appliqué à la sécurité des systèmes d'Information

M. Hedabou, ENSA de Safi ; Université Cadi Ayyad, Marrakech

10h40-11h00 : Pause Café

Chairman M. Bennai (Univ Hassan II Mohammedia)

**11h00-11h15 : Réalisation d'une porte Quantique NTCP avec des qubits
Supraconducteurs couplés au résonateur**

K. Essamouni, M. Bennai, Université Hassan II, Mohammedia

11h15-11h30 : Codes Correcteurs d'Erreurs

S. Seddik, R. Ahl Laamara, M. Daoud, N. Fahssi, LPHE-FS, Université Mohamed V-Agdal-Rabat

11h30-11h45 : Implémentation d'une porte de phase a 4 qubits dans une cavité QED

Chouikh, M. Bennai, Université Hassan II, Mohammedia

11h45-12h00 : Cryptographie Quantique avec des Variables Continues

M. Mihigo, M. Daoud, , LPHE-FS, Université Mohamed V-Agdal-Rabat

12h00-12h30 : Discussion