

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

en collaboration avec

L'ENSET-Rabat, Fac Science-Rabat et Le LPHE-Modelisation & Simulation-FSR
organisent une

Ecole Nationale

Théorie Quantique de L'Information: Fondements et applications

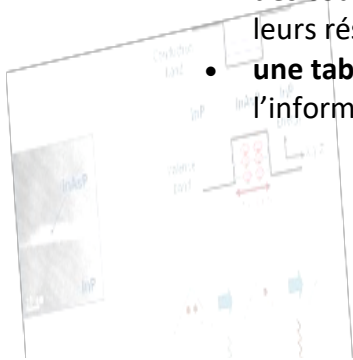
30 Novembre et **01** Décembre 2012

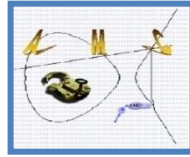
L'**Information Quantique** est un champ de recherches qui se place à l'interface de la physique, de l'informatique, des mathématiques et de la chimie. Les propriétés fondamentales de la Physique Quantique servent aujourd'hui de ressources à ce nouvel axe. Les nombres conséquents de publications, de brevets déposés, et aussi de personnels impliqués traduisent l'intérêt pour l'information quantique et sa reconnaissance comme une discipline à part entière. Elle est également à l'origine de progrès notoires, aussi bien du point de vue fondamental qu'appliqué. On trouve dans ce cadre les protocoles d'échange sécurisé d'information regroupés sous le nom générique de "cryptographie quantique" et ceux liés au traitement de l'Information Quantique connus sous le nom de "calcul quantique".

Le but principal de cette école marocaine, organisée conjointement par **Le Groupement National De Recherches - Information Quantique**, l'ENSET 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 4 modes de communication :

- **des conférences**, à caractère pédagogique soutenu, sur les fondements et les applications les plus avancées du domaine ;
- **des séminaires** sur les sujets d'actualité de l'information quantique;
- **des courtes présentations de 15 mn** afin de permettre aux plus jeunes de présenter leurs résultats à l'ensemble de la communauté;
- **une table ronde** relative à l'enseignement de la physique quantique au travers de l'information quantique et les outils mathématiques indispensables pour le domaine





Universités Mohamed V- Souissi & Agdal, L'Association Marocaine de Cryptographie
Et



Groupement National De Recherches - Information Quantique

en collaboration avec

L'ENSET-Rabat, Fac Science-Rabat et Le LPHE-Modelisation & Simulation-FSR
organisent une

Ecole Nationale



Théorie Quantique de L'Information Fondements & Applications



Thèmes

Information Quantique
Sécurité Quantique
Corrélations Quantiques
Protocoles Quantiques
Cryptographie conventionnelle
Cryptographie Homomorphique

Comité Scientifique

T.Mrabet (Président, Univ Mohamed V-Souissi)
A. Azhari (Univ Hassan II, Casablanca)
M. Daoud (Univ Ibn Zohr, Agadir)
E.H Saidi (Univ Mohamed V-Agdal, Rabat)

Comité d'Organisation

A.Azhari (Univ Hassan II, Casablanca),
C. Nacir (l'ENSET de Rabat), M. Daoud (Fac Sciences,
Agadir), R. Ahl Laamara (LPHE-MS, Fac Sciences,
Rabat), E.H Saidi (LPHE-MS, Fac Sciences, Rabat)



30 Novembre et 01 Décembre 2012
ENSET-Rabat - Fac Sciences-Rabat

PROGRAMME

Vendredi: Matinée (Amphi A, ENSET-Rabat)

08h30-09h00: Inscription

09h00-09h30 : Ouverture de l'Ecole

09h30-10h00 : Pause-café

SESSION 1 : L'Information Quantique

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

10h00-10h45 : Théorie quantique de l'information : Développements Récents

M. Daoud, FS, Université Ibn Zohr, Agadir

10h45-11h30 : Post quantum cryptography

A. Nitaj, Université Caen, France

11h30-12h15: Cryptographie quantique : Principes et applications

M. Bennai, Université Hassan II Casablanca

12h15-12h35: Etats cohérents Intriqués

El Bannany, LPHE-FS, Université Mohamed V-Rabat

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

SESSION 2 : Sécurité Quantique

Chairman M. Daoud (Univ Ibn Zohr Agadir)

14h30-15h15 : Qubits et Cryptographie

A.Azhari, Université Hassan II, Casablanca

15h15-16h00 : Enjeux en cryptographie quantique : concepts et innovations

My Hfid Hamidi, INRIA, Paris, France

16h00-16h15 : Pause-Café

SESSION 3 : Corrélations Quantiques

Chairman A. Azhari (Univ Hassan II, Casablanca)

16h15-17h00 : Intrication et discorde quantiques

M. Daoud, FS, Université Ibn Zohr, Agadir

17h00-17h20 : Mesure géométrique de la discorde quantique

R. Essaber, LPHE-FS, Université Mohamed V-Agdal-Rabat

17h20-17h40 : Intrication et transitions de phases quantiques

T. Charki, LPHE-FS, Université Mohamed V-Agdal -Rabat

17h40-18h00 : Discussions

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

SESSION 4: Protocoles Quantiques

Chairman A. Nitaj (Univ Caen, France)

09h00-09h45 : Extensions du protocole quantique BB84

M. Daoud, FS, Université Ibn Zohr, Agadir

09h45-10h30: Aspects statistiques du protocole BB84

El Hassan El Kinani, Université Moulay Ismail, Errachidia

10h30-10h45 : Pause Café

SESSION 5: Cryptographie conventionnelle

Chairman E.H El Kinani (Univ My Ismail)

10h45-11h30 : Sur la sécurité de l'information

M. Hedabou, ENSA, Université Caddi Ayyad, Safi

11h30-12h15: Post- quantum identification and signature scheme

El Youssfi El Alaoui, Darmstadt Univ, Germany

SESSION 6: Cryptographie Homomorphique

Chairman My Hfid Hamidi (INRIA, Paris, France)

12h15-13h15: Présentation des travaux de recherches des doctorants

O. Saddiki (Cloud Computing I)

M. Lamsakhar (Cloud Computing II)

Z. Jamal (Homomorphic Encryption)

A. Taibi (Torus Cryptography)

13h30: Clôture de l'école