Chaire André-Aisenstadt Chair 2011

Renato Renner

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Cette conférence s'adresse à un large auditoire / Suitable for a general audience
Cette conférence ne nécessite aucune connaissance préalable de la physique quantique / This lecture does not require prior knowledge of quantum physics

Mercredi, 12 octobre 2011, 16h30 / Wednesday, October 12, 2011, 4:30 pm
Salle – Room 1360
Centre de recherches mathématiques, Pavillon André-Aisenstadt,
Université de Montréal, 2920, chemin de la Tour

What Does Quantum Cryptography Tell Us About Quantum Physics?

Heisenberg's uncertainty principle asserts that certain observable quantities, such as position and velocity of a quantum particle, cannot be simultaneously known to arbitrary precision. More than 25 years ago, it has been realized that this feature of quantum physics can be exploited in cryptography for securely transmitting secret messages over insecure channels. Since this discovery, research in the emerging area of quantum cryptography has resulted in a variety of remarkable insights on the nature of information. In my talk, I will show how these insights influence our understanding of physics. In particular, using cryptographic considerations, I will argue that quantum physics is the most informative theory that is compatible with experimental observations and therefore, in a certain sense, complete.

Une réception suivra la conférence au
Salon Maurice-L'abbé, Pavillon André-Aisenstadt (Salle 6245)
There will be a reception after the lecture in
Salon Maurice-L'abbé, Pavillon André-Aisenstadt (Room 6245)

Conférence dans le cadre de l'atelier sur l'informatique quantique
Lecture at the Workshop on Quantum Computer Science

Mercredi, 5 octobre 2011, 16h00 / Wednesday, October 5, 2011, 4:00 pm
Salle – Room 6214
Centre de recherches mathématiques, Pavillon André-Aisenstadt,
Université de Montréal, 2920, chemin de la Tour

Free Randomness Amplification

Assume that we have access to a source of weakly random bits, with the only guarantee that the entropy of each bit (conditioned on all previously available information) is above a certain threshold. In 1984, Santha and Vazirani showed that, in a purely classical setting, it is impossible to amplify the quality of such a source. More precisely, there is no (deterministic) function that transforms weakly random bits into (almost) uniform ones. In this talk, I will consider a quantum-physical scenario and show that, using entanglement, the amplification of weakly random sources becomes possible. An interesting implication of this result is that no perfect randomness is required for applications such as cryptography or for Bell tests.

Conférence dans le cadre de l'atelier sur l'information quantique et la physique statistique
Lecture at the Workshop on Quantum Information in Quantum Many-body Physics

Jeudi, 20 octobre 2011, 16h00 / Thursday, October 20, 2011, 4:00 pm
Salle – Room 6214
Centre de recherches mathématiques, Pavillon André-Aisenstadt,
Université de Montréal, 2920, chemin de la Tour

An Information-Theoretic View on Thermalization

How can the reversible dynamics of physical processes give rise to irreversible phenomena such as thermalization? I will reconsider this old question using modern tools from quantum information theory. In particular, I will show how recently developed techniques, such as the decoupling approach to quantum information, allow us to make quantitative statements about the thermalization properties of physical systems.

www.crm.math.ca/Renner

22-09-2010