SEMINARIO

Security via Uncertainty:
The Amazing Resources of Quantum Physics

Fabio Antonio BOVINO
Quantum Optics Lab Selex-ES Finmeccanica

Venerdì 15 Novembre 2013 - ore 14.30

AULA SEMINARI- Dip. Scienze di Base e Applicate per l'Ingegneria
Pal. E - Via Scarpa 16 -ROMA

At the beginning of the cryptography, the security of a decoder depended on the secretiveness of the whole procedure of encryption and decryption. In modern cryptography these two operations are of public dominion, but the key is maintained secret. Claude Shannon has shown that a message can unconditionally be protected from attempts of espionage thanks to systems as that of Vernam (One-Time-Pad), in which the key is as long as the message, it is entirely random and is used only one time.

Nevertheless, the oldest and more delicate problem connected to conventional encryption systems, both "classical" and "modern", remains the management of the keys, including the generation, the possible maintenance and the dispatch to the legitimate recipients. A security loss in each of these steps, can jeopardize the whole structure. Actually, the management of the keys represents the true Achille's heel of every cryptographic system.

Quantum cryptography offers new methods of secure communication that are not threatened even by the power of computers. Unlike classical cryptography, it relies on the laws of physics rather than on ensuring that successful eavesdropping would require excessive computational effort.
Quantum Physics can deliver **«correlations with promises»**. In particular, it can distribute at two locations strictly correlated strings of bits, with the promise that no copy of these bits exist anywhere in the universe. This promise is guaranteed by the laws of Nature, and does not depend on any mathematical assumption. Consequently, such two strings of correlated bits provide perfect secure keys, ready to be used in standard cryptosystems.

Fabio Antonio Bovino was employed at Elsag, a Finmeccanica Company, in September 2001 (at Selex-ES from January 2013). He is the founder and the chief scientist of Quantum Optics Lab. He has participated in national and international research projects financed by MIUR, Italian Ministry of Defense, and European Community. He is author of more the 80 publications in national/international journals, and 12 patents in the fields of Foundation of Quantum Mechanics, Quantum Optics, Quantum Information and Computing. Highlights are the first demonstration of a quantum cloning machine (2001), the first experiment beyond Bell's Inequalities for entanglement characterization (2004), the realization of the first Quantum Cryptography Italian product: the Q-KeyMaker®. He is Lecturer at ICTP "The Abdus Salam International Centre for Theoretical Physics" and at Ettore Majorana Foundation and Centre for Scientific Culture, where he was, in 2012, Director of Course "Advances in Nanophotonics". He is member of the teaching and scientific board of the Second Level Master on Optics and Quantum Information of the University of Rome "Sapienza".
Personal WebSite http://it.linkedin.com/in/fabioantoniobovino

Tutti gli interessati sono invitati a partecipare

Per informazioni:
Dip.SBAI – Univ. 'La Sapienza'
Tel 06.49766541- concita.sibilia@uniroma1.it