



Course on

Cryptography

September 1-2, 2016

Room A212, Polo Scientifico e Tecnologico Fabio Ferrari (Povo 1)

- The course aims to introduce to modern cryptography, with particular focus on applications, the role of entropy, and the role of quantum mechanics
- The target audience is post-docs and PhD students involved in the project SiQuro. Other collaborators are also invited to participate.
- The course is free, but subscription is mandatory.
- Travel, accommodation and meal expenses are not reimbursed by the organizers.

Program

Thursday, September 1, 2016

14:00-14:45 *Cryptographic primitives*, Prof. Massimiliano Sala

15:00-15:45 *Applications of cryptography* Dr. Michela Ceria

16:00-16:45 *Randomness in cryptographic primitives*, Dr. Massimiliano Sala

17:00-17:45 *Randomness in applications of cryptography* Dr. Matteo Piva

Friday, September 2, 2016

09:00-09:45 *Limitations of classical cryptography*, Prof. Massimiliano Sala

10:00-10:45 *Foundations of Quantum Cryptography* Dr. Davide Pastorello

11:00-11:45 *QKD protocols: BB84, EE91*, Dr. Davide Pastorello

12:00-12:45 *Advanced topics in QC*, Dr. Davide Pastorello