CTIC workshop:
Quantum Information & Quantum Cryptography
October 19-23, 2015
Aarhus University, Denmark

Title: **Classical leakage resilience from quantum fault tolerance**

Felipe Lacerda

Physical implementations of cryptographic algorithms leak information, which makes them vulnerable to so-called side-channel attacks. The problem of secure computation in the presence of leakage is generally known as leakage resilience. I'll show a connection between leakage resilience and fault-tolerant quantum computation. This is done in two steps: (i) proving that for a general leakage model, there exists a corresponding noise model in which fault tolerance implies leakage resilience, and (ii) showing how to use constructions for fault-tolerant quantum computation to implement classical circuits that are secure in specific leakage models.