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

Title: From Bell inequality violations towards device independence of general quantum cryptographic protocols

Stephanie Wehner

Bell tests form an essential ingredient for device independent quantum cryptography. Recently, the elusive goal of performing a loophole free Bell test has finally been achieved by using entangled electron spins in diamond. We start by reporting on this experiment, before proceeding to develop the theory of device-independent two-party quantum cryptography. Concretely, we propose a model and protocol for device-independent weak string erasure in the bounded and noisy-storage model that can in turn be converted to other protocols such as bit commitment. Finally, we prove its security against sequential attacks.

Joint work with
Experiment:
B. Hensen, H. Bernien, A. Dreau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R.F.L. Vermeulen, R.N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D.J. Twitchen, D. Elkouss, S. Wehner, T.H. Taminiau, R. Hanson - 1508.05949, To appear in Nature.

Theory:
J. Kaniewski, T. Vidick, S. Wehner - In preparation.