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

Title: The orthogonal vector problem

Ivan Damgård

In the orthogonal vector problem two parties A and B do an interactive protocol with the goal of outputting two random vectors, u for A and v for B, such that uv=0, while maintaining certain privacy properties against an external adversary. We show that there is no classical protocol that solves this, but that there is a quantum solution. We also look at application of the quantum protocol for leakage resilient crypto.

Joint work with Fred Dupuis and Jesper Nielsen