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

Title: Local, Entangled and Non-Signaling Zero-Knowledge Multi-Prover Interactive Proofs

Claude Crépeau

Several Zero-Knowledge Multi-Prover Interactive Proof Systems found in the litterature claim soundness that is actually missing. This situation was first observed in \cite{CSST11} where a notion of {\em Provers Isolation} is defined to address such issues. We discuss a number of existing zero-knowledge interactive proof systems and demonstrate that they do not satisfy even a weak isolation condition. We provide a proof that every language in $\mathbf{MIP}$ has a Zero-Knowledge Multi-provers Interactive Proof System. We consider extensions to languages in $\mathbf{NEXP} \subseteq \mathbf{MIP}^{\star}$ for Zero-Knowledge Entangled Multi-provers Interactive Proof Systems and finally, we show that languages in $\mathbf{MIP}^{\mathbf{ns}}$ cannot have Zero-Knowledge No-Signaling Interactive Proof Systems at all.