Quantum Communication Attacks on Classical Cryptographic Protocols

(Invited Talk)

Ivan Damgård

Dept. of Computer Science, Aarhus University

Abstract. In the literature on cryptographic protocols, it has been studied several times what happens if a classical protocol is attacked by a quantum adversary. Usually, this is taken to mean that the adversary runs a quantum algorithm, but communicates classically with the honest players. In several cases, one can show that the protocol remains secure even under such an attack.

However, there are also cases where the honest players are quantum as well, even if the protocol uses classical communication. For instance, this is the case when classical multiparty computation is used as a “subroutine” in quantum multiparty computation. Furthermore, in the future, players in a protocol may employ quantum computing simply to improve efficiency of their local computation, even if the communication is supposed to be classical. In such cases, it no longer seems clear that a quantum adversary must be limited to only classical communication with the honest players. And so the natural question is: what happens to the security if this limitation is dropped?

In this talk, we survey some results from ongoing work that addresses this question, more specifically, we consider security of secret sharing, zero-knowledge protocols and multiparty computation under this new paradigm. In all cases, both positive and negative results can be shown. For instance, a classical threshold secret sharing scheme designed for threshold t is no longer secure in this model, but the same scheme *is* secure with threshold $t/2$.

This is joint work with Jakob Funder, Jesper Buus Nielsen (Dept. of Computer Science, Aarhus University) and Louis Salvail (Université de Montréal).