Definition & Application of Quantum Zero-Knowledge proofs & VQSS

Claude Crépeau
School of Computer Science
McGill University
Pavillon McConnell, 3480, rue University
Montréal, Québec
CANADA H3A 2A7

Abstract

We present a perfect zero-knowledge proof system for proving the correctness of the distribution of shares in a Quantum Secret Sharing scheme under a straightforward generalization of the classical definition of Zero-Knowledge to the quantum world. This multiparty situation is the only scenario known so far where this stragihtforward but demanding definition may be satisfied. We then use this proof system to construct a Verifiable Quantum Secret Sharing (VQSS) scheme.

Joint work with Adam Smith and Dan Gottesman.