SARAH PLOSKER, University of Guelph

Private Quantum Codes

Private quantum codes are a basic tool in quantum key distribution and quantum cryptography. We define private quantum channels mathematically, and consider a general notion of private quantum codes wherein qubits are encoded into quantum subsystems. Private quantum channels, private subspaces, and a previously considered notion of private subsystems are all captured as special cases of this general phenomena. We provide a simple example that highlights the main differences between mappings on subsystems and subspaces and show that certain classes of channels can only be private in this subsystem setting. We also set out testable conditions for deciding when a code is private for a given channel and we discuss connections with quantum error correction. These conditions can be regarded as the private analogue of the Knill-Laflamme conditions for quantum error correction. Joint work with T. Jochym-O'Connor, D. W. Kribs, and R. Laflamme.