Classical and quantum fingerprinting

Abstract: Fingerprinting enables two parties to infer whether the messages they hold are the same or different when the cost of communication is high: each message is associated with a smaller fingerprint and comparisons between messages are made in terms of their fingerprints alone. We review known results in classical and quantum fingerprinting, showing that in the scenario where the two parties are forbidden access to a public coin, fingerprints constructed from quantum information can be made exponentially smaller than those constructed from classical information. We then give specific constructions of optimal classical fingerprinting strategies when access to a public coin is granted, and show how shared entanglement enables quantum strategies to outperform them.