

Classical and quantum fingerprinting strategies

Andrew Scott¹, Jonathan Walgate and Barry Sanders
Institute for Quantum Information Science
University of Calgary, Calgary, Alberta T2N 1N4, Canada
e-mail: ¹ascott@qis.ucalgary.ca

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. When the two parties are forbidden access to a public coin, it is known that fingerprints composed of quantum information can be made exponentially smaller than those composed of classical information. We present specific constructions of classical fingerprinting strategies through the use of constant-weight codes and provide bounds on the worst-case error probability with the help of extremal set theory. These classical strategies are easily outperformed by quantum strategies constructed from equiangular tight frames.