Rewinding-Free Quantum Security Reductions

Donald Beaver
Seagate Technology
920 Disc Drive
Scotts Valley, CA 95066
U.S.A.

Abstract

The possibility that quantum key exchange can be information-theoretically private yet bind the sender and receiver to the secret message they exchanged presents a number of difficulties to achieving quantum reductions in which rewinding is disallowed. Yet rewinding presents its own conundrum: it allows the otherwise physically illegal cloning and extraction of quantum information. Some results on avoiding binding in quantum key exchange will be presented, facilitating a rewinding-free approach in the quantum setting. Also, related observations on the new and unexpectedly more invasive nature of quantum attacks will be presented.