Quantum state targeting

Terry Rudolph rudolpht@bell-labs.com Bell Labs, 600-700 Mountain Ave., Murray Hill, NJ 07974, U.S.A. Robert W. Spekkens rspekkens@perimeterinstitute.ca Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2J 2W9, Canada

abstract We introduce a new primitive for quantum communication that we term "state targeting" wherein the goal is to pass a test for a target state even though the system upon which the test is performed is submitted prior to learning the target state's identity. Success in state targeting can be described as having some control over the outcome of the test. We show that increasing one's control above a minimum amount implies an unavoidable increase in the probability of failing the test. This is analogous to the unavoidable disturbance to a quantum state that results from gaining information about its identity, and can be shown to be a purely quantum effect. We provide some applications of the results to the security analysis of cryptographic tasks implemented between remote antagonistic parties. Although we focus on weak coin flipping, the results are significant for other two-party protocols, such as strong coin flipping, partially binding and concealing bit commitment, and bit escrow. Furthermore, the results have significance not only for the traditional notion of security in cryptography, that of restricting a cheater's ability to bias the outcome of the protocol, but also on a novel notion of security that arises only in the quantum context, that of cheat-sensitivity. Finally, our analysis of state targeting leads to some interesting secondary results, for instance, a generalization of Uhlmann's theorem and an operational interpretation of the fidelity between two mixed states.