CORR 2001-47

Linking Classical and Quantum Key Agreement: Is There a Classical Analog to Bound Entanglement?

Nicolas Gisin*, Renato Renner*, Stefan Wolf

Abstract After carrying out a protocol for quantum key agreement over a noisy quantum channel, the parties Alice and Bob must process the raw key in order to end up with identical keys about which the adversary has virtually no information. In principle, both classical and quantum protocols can be used for this processing. It is a natural question which type of protocols is more powerful. We show that the limits of tolerable noise are identical for classical and quantum protocols in many cases. More specifically, we prove that a quantum state between two parties is entangled if and only if the classical random variables resulting from optimal measurements provide some mutual classical information between the parties. In addition, we present evidence which strongly suggests that the potentials of classical and of quantum protocols are equal in every situation. An important consequence, in the purely classical regime, of such a correspondence would be the existence of a classical counterpart of so-called bound entanglement, namely "bound information" that cannot be used for generating a secret key by any protocol. This stands in contrast to what was previously believed. The studied connection between the classical and quantum protocols makes it natural to conjecture that (classical and quantum) distillability is possible only if single-copy distillability is already possible.

Keywords Secret-key agreement, intrinsic information, secret-key rate, purification, entanglement.