The Physical Underpinning of Security Proofs for Quantum Key Distribution

Jean Christian Boileau
Ph.D. (Institute for Quantum Computing, Univ. of Waterloo and Perimeter Institute, Waterloo)
Fellow, Center for Quantum Information and Quantum Control
University of Toronto
e-mail: jc.boileau@utoronto.ca

Physical concepts associated with quantum mechanics, like the uncertainty principle or entanglement, paved the way to the first successful security proof for QKD. Ever since, further development in security proofs for QKD has been remarkable. But the connection between entanglement distillation and the uncertainty principle has remained obscured by the mathematics. Our main goal is to dig the physics out of the new advances in security proofs for QKD.

It is well-known that every quantum key distribution (QKD) protocol corresponds to some private state distillation protocol, where private state is defined as some twisted maximally-entangled state. Recently, Koashi uncovered the general role of complementarity in security proofs for QKD. In this paper, we emphasize the definition of private states in term of an uncertainty principle between two complementary observables. We extend this idea to imperfect private states and, in this new framework, give a more intuitive proof of Devetak and Winter's secret key generation rate for symmetrized quantum states. This greatly clarifies the distinctions and similarities between different methods (i.e. reducing to a distillation protocol, exploiting some uncertainty principle or building upon more information-theoretic arguments) for proving security for QKD.

We also discuss a generic security proof for one-way permutation-invariant QKD protocols, and show how to build a shield from bit error correction. The latter generalizes an observation from Kraus, Branciard and Renner to improve the secret key generation rates of SARG04 by considering a different symmetrization. In certain situations, we argue that Azuma's inequality can simplify the security proof considerably, and we discuss the implications for finite key length QKD of reducing a protocol to an entanglement or a more general private state distillation protocol.

(Joint work with Joseph M. Renes)