Abstract

Quantum theory provides the ground for the most significant technological advances of the twenty-first century. The quantum revolution that is about to happen will bring us not only quantum computers but also quantum communication between quantum hardware. The global network of quantumly communicating devices will constitute the so-called quantum Internet. The promise quantum theory brings us about quantum communication is higher than the classical level of security and, in some scenarios, even unconditional security. Namely, there exist protocols for secret key distillation having entangled quantum states as a resource such that the security of the produced secret key is guaranteed by the laws of physics and are independent of the (possibly malicious) inner-working of the involved cryptographic devices. The more bits of the secure key can be distilled, given some entangled resources, the better the performance of the protocol. In this way, particular protocols constitute the lower bounds on the key rate achievable in the scenario. On the other hand, determining the optimal protocol or justification for pursuing it requires knowledge of the upper bounds on the achievable key rate. Finding the upper bounds on the secure key rate is, therefore, of crucial importance regarding the construction of quantum communication networks of the future.

In the collection of articles constituting this dissertation, of which I am a coauthor, as our primary interest, we study the fundamental limitations within the selected quantum and supra-quantum cryptographic scenarios in the form of upper bounds on the achievable key rates. We investigate various security paradigms, bipartite and multipartite settings, as well as single-shot and asymptotic regimes. Specifically, our findings contribute to the secret key agreement scenario (SKA), device-dependent conference key agreement scenario (DD-CKA) both for quantum channels and quantum states in one-shot and asymptotic regimes, device-independent conference key-agreement scenario (DI-CKA) in both asymptotic and one-shot regime, and non-signaling device-independent secret key agreement scenario (NSDI). Our studies, however, extend beyond the derivations of the upper bounds on the secret key rates in the mentioned scenarios. In particular, we propose a novel type of rerouting attack on the quantum Internet for which we find a countermeasure and benchmark its efficiency. Furthermore, we propose several upper bounds on the performance of quantum (key) repeaters settings. We derive a lower bound on the secret key agreement capacity of a quantum network, which we tighten in an important case of a bidirectional quantum network. The squashed nonlocality derived here as an upper bound on the secret key rate is a novel non-faithful measure of nonlocality. Furthermore, the notion of the non-signaling complete extension arising from the complete extension postulate as a counterpart of purification of a quantum state allows us to study analogies between non-signaling and quantum key distribution (QKD) scenarios.

From a larger perspective, our results are not only technical ones describing selected cryptographic tasks. In some cases, our findings confront fundamental questions regarding the foundations of quantum theory. The frameworks we develop allow to investigate this underlying subject insightfully both from the inside and outside of the quantum theory.