SEMINAR: Updates on the Bound Key Conjecture

STEFAN BAUML

September 08, 2026
11:00 to 12:00
Blue Lecture Room

A long standing open problem in the theory of quantum resources is whether there exist states that need quantum key as a resource when being created using only local operations and classical communication (LOCC), but from which no quantum key is obtainable using only LOCC. Motivated by the analogous term in entanglement theory such states would be called bound key states. A related question is whether there exist entangled states from which no cryptographic key can be distilled, or conversely whether the distillable key is faithful as a measure of entanglement. We refer to such states mathematical bound key. In this work we shed some light on those questions, discussing the non-triviality of defining a measure of key cost in analogy to the entanglement cost.
We provide show a surprising dichotomic relationship between the existence of mathematical bound key and an asymptotic version of the bound key conjecture. We also generalise the concept of bound key to the multipartite setting of conference key agreement and discuss ways in which a key cost can be defined. We show that there exist multipartite entangled states which cannot increase the key of any other state when provided as an additional resource. We further provide a lower bound on the dimension a bound entangled state needs to have to be close to a private state in trace distance, which indicates a non-negligible memory cost of networks safe from certain attack on its nodes.
Hosted by: Prof. Dr. Antonio Acin