Università della Svizzera italiana
Faculty of Informatics

Bound Information: analysis on the classical analog to Bound Entanglement

Student: Luca Dolfi **Advisor:** Prof. Stefan Wolf **Assistant:** Arne Hansen

Abstract

There is a correspondence between entanglement distillation in quantum mechanics and classical key agreement in information theory. In the quantum-mechanical framework there are, furthermore, non-distillable, but entangled quantum states. So, considering the above analogy, does there exists some notion of bound information? As of today this remains an open question.

In this project we follow the intuition from bound entanglement, the related measures and their connections to concepts of classical key agreement, as well as related information-theoretical concepts, in order to further investigate this open question.
We also look at a candidate probability distribution for bound information and perform numerical simulations in search for new, possibly better, candidates for bound information.

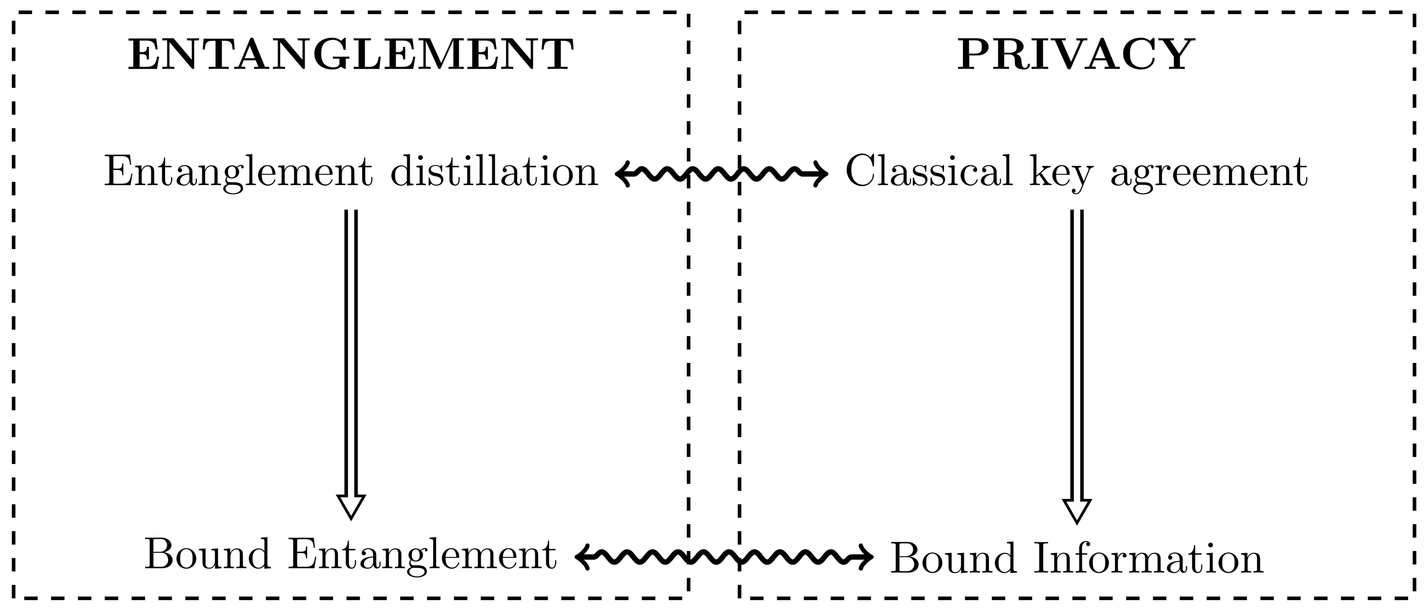
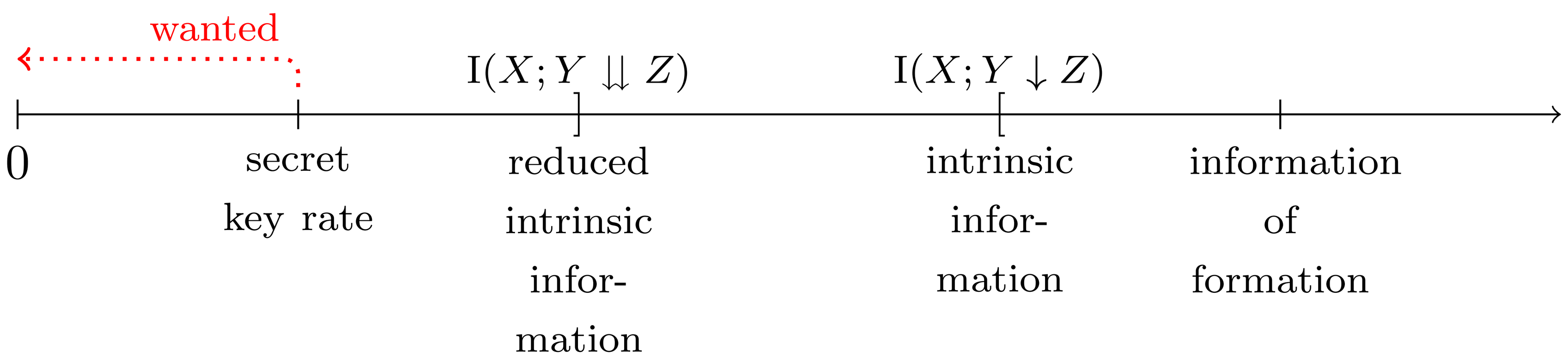


Fig. 1 *Some aspects of quantum mechanics can be mapped to classical information theory*



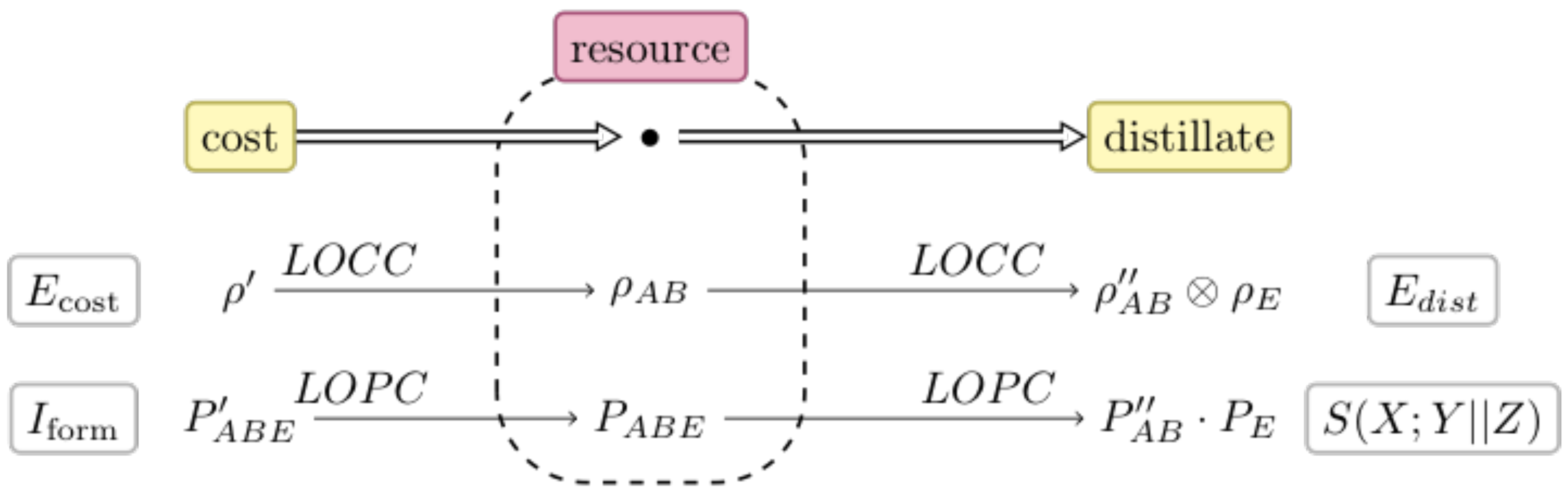


Fig. 2 *Entanglement distillation and CKA have similar concepts of resource, cost and distillate*

The **secret key rate** $S(X;Y\|Z)$ is defined as the maximal amount of correlated bits between Alice and Bob extractable from an arbitrarily large number of realisations of a distribution P_{XYZ}, through a protocol using LOPC, such that Eve has no information about them, i.e. she is factored out.

The **information of formation** $I_{form}(X;Y|Z)$ of X and Y, given Z, is the rate at which initial secret bits are required to synthesise a distribution which is, in terms of privacy, at least as good as P_{XYZ} from Alice and Bob's point of view, and where the piece known to Eve, Z, is derived from the entire public communication of the protocol.

Entanglement distillation and CKA

To measure entanglement one might consider the maximal number of singlets that can be *distilled* from ρ by local operations and classical communication (LOCC). Bound entangled states are states that require a number of singlets for their preparation while they, in turn, do not allow to distill any singlets.

Similarly, in classical key agreement, there is the idea of the amount of perfectly secret bits required to synthesise a certain probability distribution by local operations and public communication (LOPC).

Bound Information

The counterpart to bound entanglement, is a kind of correlation which can not be used for generating a secret key.

> *Is there a tripartite probability P_{XYZ}, corresponding to Alice and Bob wanting to establish a key unknown to Eve, that has non-zero key cost, while not allowing to distill any secret key (zero secret key rate but non-zero information of formation)?*

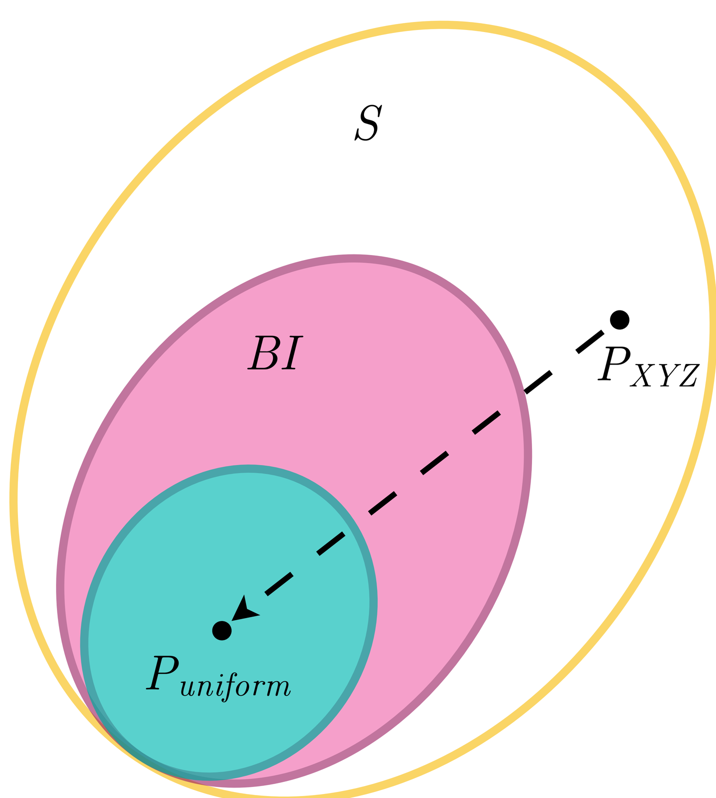


Fig. 4 *From the set S of distributions with extractable key we create a "path" towards distributions with zero key cost*

Fig. 5 *Graph showing results*

A candidate distribution

Analogously to bound entanglement, we applied different noise functions (represented as "paths" in Fig. 4) to a probability distribution from literature and measured for each step the values of *reduced* and normal *intrinsic information*, as well as tests for *separability* of the translated quantum state.
We opted for a Monte Carlo method to calculate the infima of the information theoretical values.