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

One can show that there exists a correspondence between entanglement distillation in quantum mechanics and classical key agreement in information theory. In the same 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 remain an open question.
In the project we follow the intuition of 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.

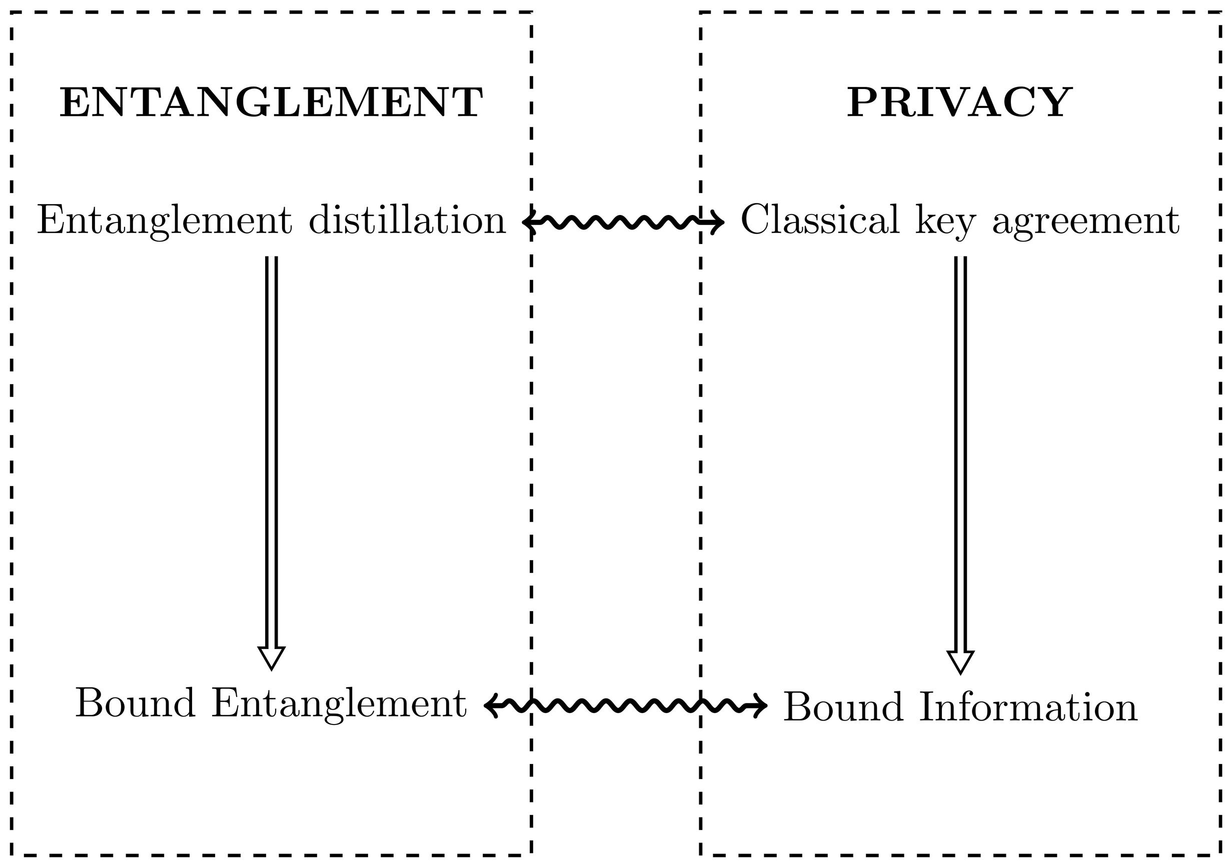


Fig. 1 *Some aspects of quantum mechanics can be mapped to classical information theory*

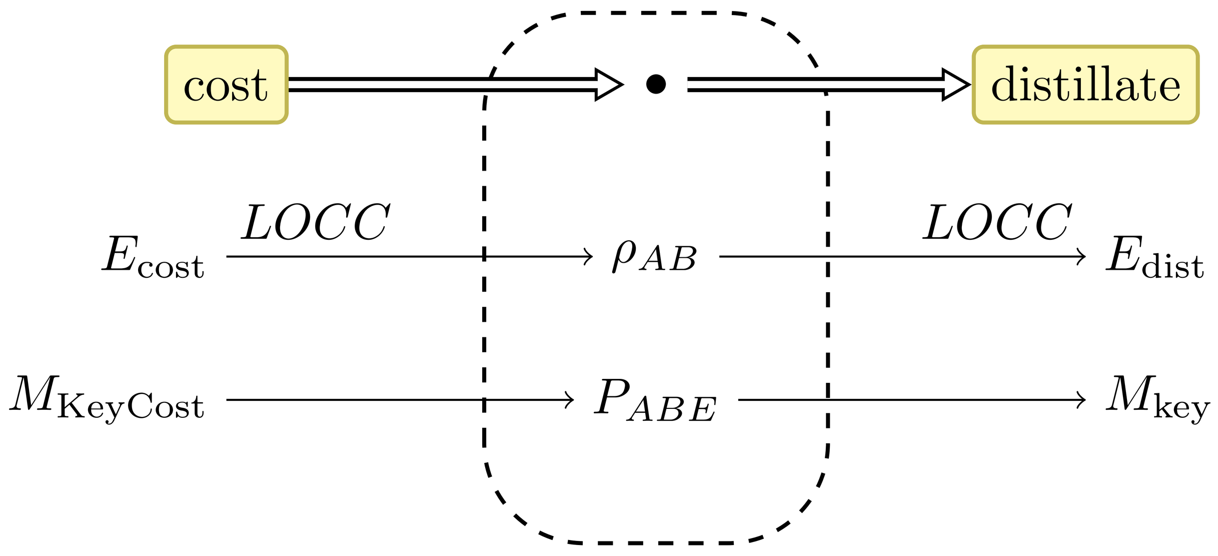
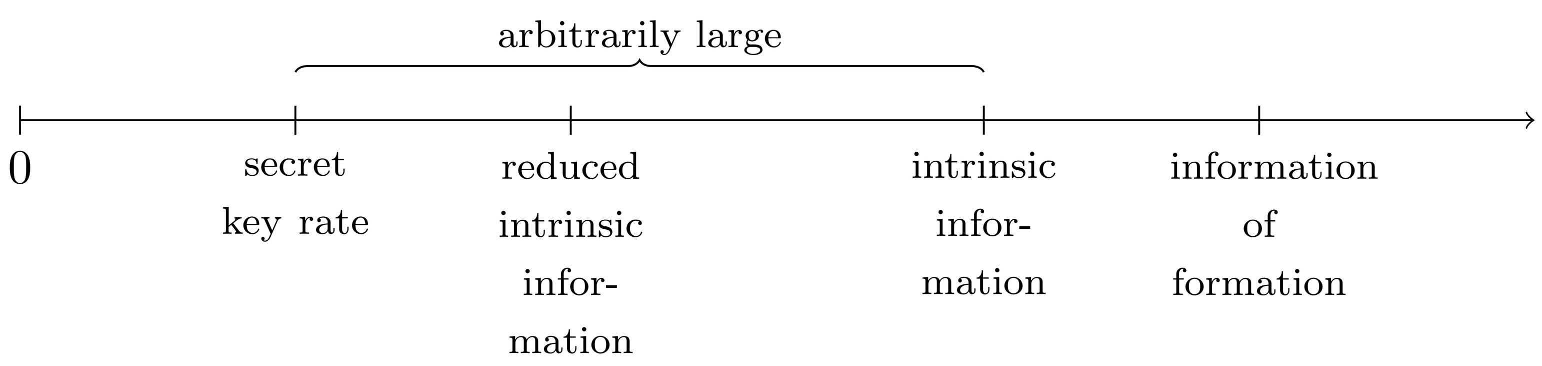


Fig. 2 *Quantum distillation and CKA have similar concepts of resource and distillate*

$S(X;Y\|\|Z)$	***Secret key rate***: the amount of extractable secret correlation from P_{XYZ}
$\mathrm{I}(X;Y\downarrow Z) := \inf_{Z\to\bar{Z}} \mathrm{I}(X;Y\|\bar{Z})$	**Intrinsic information**: the remaining correlated secrecy after Eve's best choice of a viewpoint
$\mathrm{I}(X;Y\downarrow\downarrow Z) := \inf_{P_{U\|XYZ}} (\mathrm{I}(X;Y\downarrow ZU) + \mathrm{H}(U))$	**Reduced intrinsic information**: a stricter upper bound to secret key rate



Bound Information

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

- Is there a tripartite probability P_{XYZ}, that has some *cost* associated to it to create it, but has 0 possible key bits distillable from it?

Bound entanglement is a kind of correlation between Alice and Bob inaccessible to Eve but nevertheless of no use for generating a secret key.

$Y \backslash X$	0	1	2	3
0	1/8	1/8	a	a
1	1/8	1/8	a	a
2	a	a	1/4	0
3	a	a	0	1/4

$$Z \equiv X + Y \ (mod\, 2) \ \text{ if } X, Y \in \{0,1\}$$

$$Z \equiv X \ (mod\, 2) \ \text{ if } X, Y \in \{2,3\}$$

$$Z = (X,Y) \text{ otherwise}$$

Fig. 4 *Probability distribution (for a≥0, to be renormalised) for which S(X; Y ||Z) ≠ I(X; Y ↓ Z)*

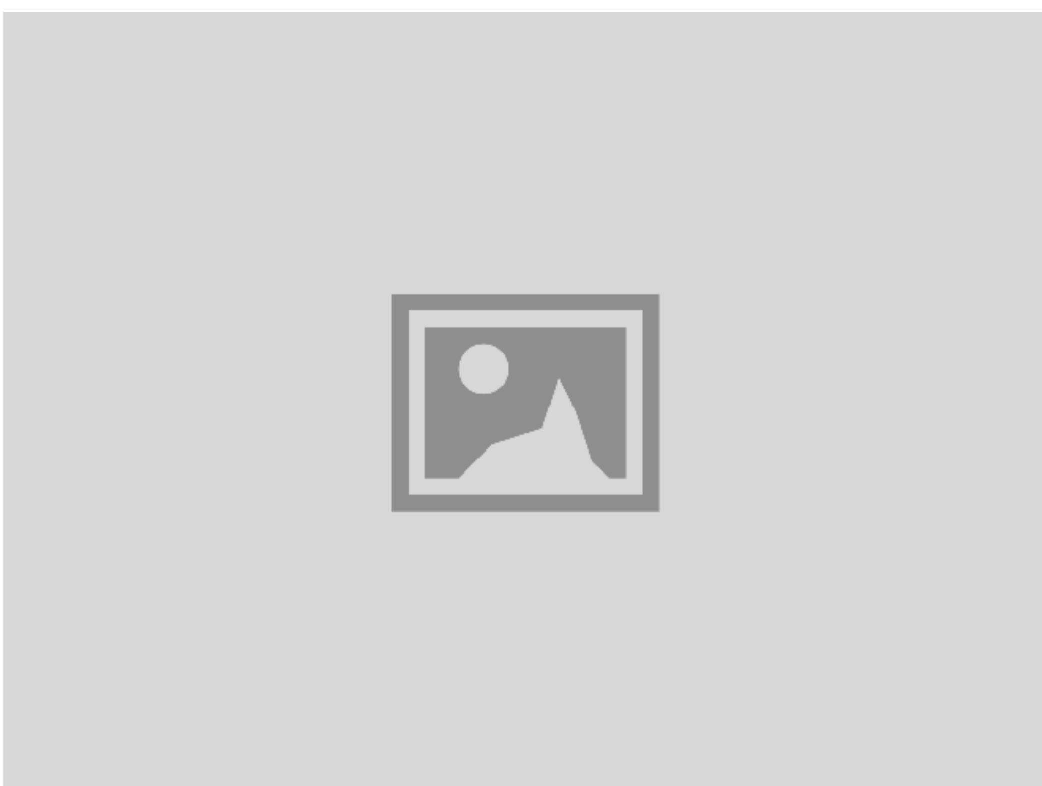


Fig. 5 *Graph showing results*

A candidate distribution

We implemented a numerical analysis of the probability distribution given in Fig. 4 in search for bound information. This probability distribution was firstly proposed by Wolf and Renner in 2003.
Analogously to bound entanglement, we applied different noise functions to the distribution and measured for each steps the values of *reduced* and normal *intrinsic information*, as well as tests for *separability* of the translated quantum state.
The graph shows the results for ...