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.

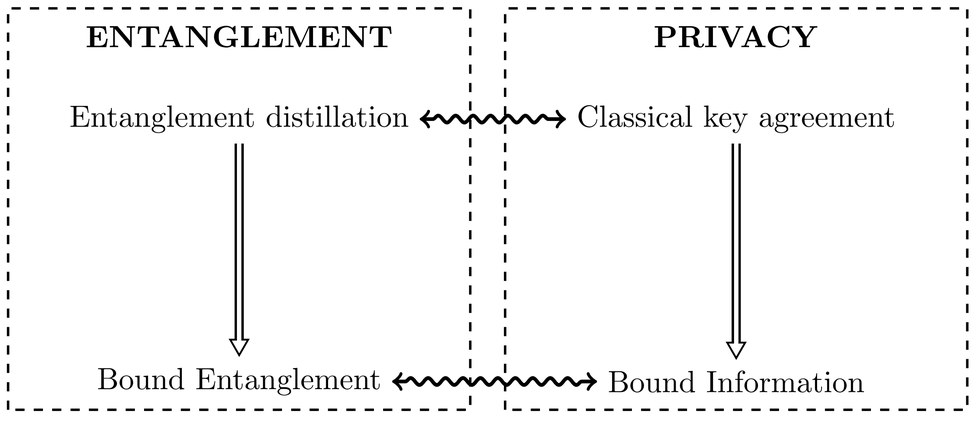
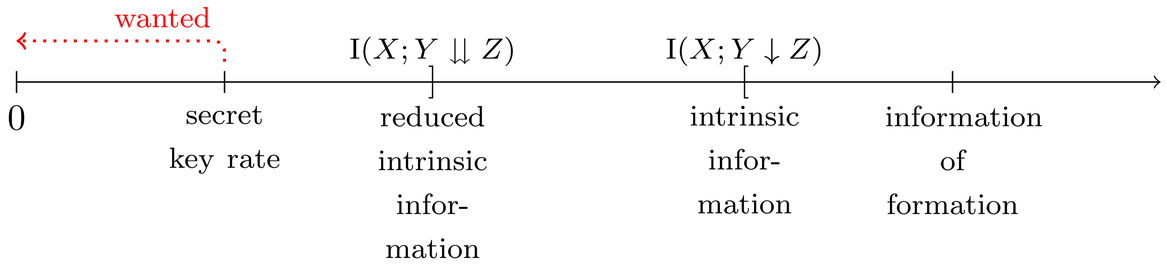


Fig. 1 *Certain aspects of quantum mechanics can be mapped to classical information theory*



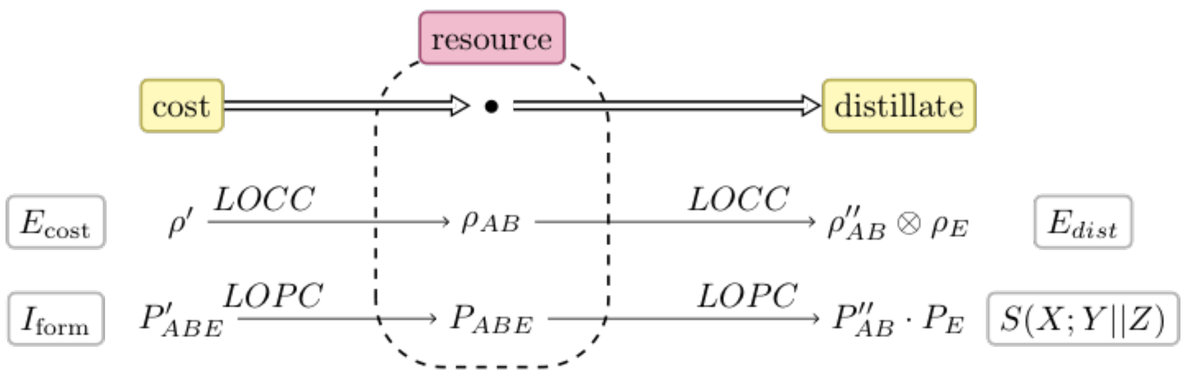


Fig. 2 *Entanglement distillation and CKA utilise a resource (mixed state or probability distribution) to produce a distillate that factors out Eve.*

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** $I_{\text{form}}(X;Y|Z)$ 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

Maximally entangled states held between Alice and Bob after a distillation protocol are—by the monogamy of entanglement—not entangled with the environment. In other words, the state Alice and Bob have is product with the environment.
The joint probability distribution P_{ABE} falls similarly into a product $P_{\text{AB}} \cdot P_E$ after a CKA protocol.

Bound Information

Bound entangled states are states that require a number of maximally entangled singlets for their preparation while they, in turn, do not allow to distill any singlets. The counterpart to bound entanglement is a kind of correlation which does not allow to extract any key from it.

> *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)?*

Problems/Conclusion

To test the simulations on the probability distributions we relied on bounds for *secret key rate* and *information of formation* given in [RW03]. However, the reduced intrinsic information resulted problematic to use since we even questioned its applicability as a general bound to prove the existence of BI.
Furthermore the BE–BI analogy seems useful on an intuitive level, but not so much on a formal level. The translation of tools—as for separability of quantum states—is not direct, considering that BE is defined on a *bipartite* state, while BI is characterised by a *tripartite* distribution.

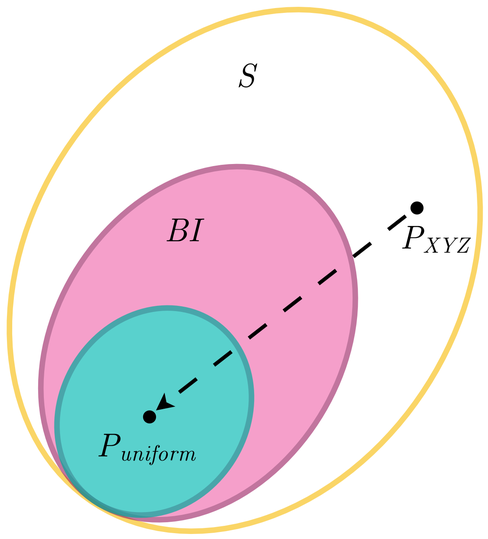


Fig. 4 *From the set* S *of tripartite distributions we create a "path" towards distributions with zero key cost (cyan), going through the ones without extractable key (magenta).*

A candidate distribution

Analogously to bound entanglement, we applied different noise functions (represented as "paths" in Fig. 4) to a probability distribution and measured, for each step, the values of *reduced intrinsic information* and *intrinsic information*, as well as tests for *separability* of the translated quantum state.

References

[RW03] Renato Renner and Stefan Wolf. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2003, pp. 562–577.

[GW00] Nicolas Gisin and Stefan Wolf. In: *Annual International Cryptology Conference*. Springer. 2000, pp. 482–500.