Master in Photonics – "PHOTONICS BCN"
ERASMUS+ "EUROPHOTONICS"

MASTER THESIS PROPOSAL

Dates: April - September 2020

Laboratory: Quantum Information Theory Group
Institution: ICFO – The Institute of Photonic Sciences
City, Country: Castelldefels (Barcelona), Spain

Title of the master thesis: Semi-device-independent randomness amplification and expansion

Name of the master thesis supervisor: Gabriel Senno, Antonio Acín
Email address : gabriel.senno@icfo.eu, antonio.acin@icfo.eu
Phone number : +34 935534060
Mail address : Av. Carl Friedrich Gauss, 3
08860 Castelldefels (Barcelona), Spain

Keywords : quantum correlations, randomness amplification and expansion, quantum entropy.

Summary of the subject (maximum 1 page):

The protocols to 1) transform an arbitrarily weak public source of randomness into an almost perfect and private one [1], and 2) generate an unbounded amount of private randomness from a finite random seed [2] are amongst quantum information theory's greatest achievements. In these protocols, a successful execution is certified by the observation of a Bell inequality violation, in a manner which is independent of the particular quantum state and measurements giving rise to such a violation. This device-independence (DI), however, comes with a price: the necessity of preparing entangled quantum states and of performing loophole-free Bell tests. In turn, this implies that, with the current technology, very low randomness generation rates can be practically achieved.

The semi-DI approach aims at retaining the conceptual advantages of DI schemes, while making their implementation technologically less challenging. The entanglement-based setup featuring in DI protocols is replaced by a prepare-and-measure one, with some type of restriction on the prepared states (bounds on Hilbert space dimension [3], fidelity [4] or average energy [5], etc.).

The goal of this master project is to design semi-DI protocols for randomness amplification and expansion and prove its information-theoretic security. Given existent results in quantum information theory, such proofs boil down to lower-bounding the von Neumann entropy of the outcomes of such protocols conditioned on any state that a quantum memory held by a malicious adversary and, potentially, entangled with the protocols' devices can have. We will be looking for, both, numerical (semidefinite programming) as well as analytical results.

References

[1] Gallego, R., Masanes, L., De La Torre, G., Dhara, C., Aolita, L., & Acín, A. (2013). Full randomness from arbitrarily deterministic events. *Nature communications*, *4*(1), 1-7.

[2] Coudron, M., & Yuen, H. (2014, May). Infinite randomness expansion with a constant number of devices. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing* (pp. 427-436).

[3] Li, H. W., Yin, Z. Q., Wu, Y. C., Zou, X. B., Wang, S., Chen, W., ... & Han, Z. F. (2011). Semi-device-independent random-number expansion without entanglement. *Physical Review A*, *84*(3), 034301.

[4] Brask, J. B., Martin, A., Esposito, W., Houlmann, R., Bowles, J., Zbinden, H., & Brunner, N. (2017). Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *Physical Review Applied*, *7*(5), 054018.

[5] Van Himbeeck, T., Woodhead, E., Cerf, N. J., García-Patrón, R., & Pironio, S. (2017). Semi-device-independent framework based on natural physical assumptions. *Quantum*, *1*, 33.

Additional information:

* Required skills : knowledge of quantum theory and some programming language.
* Miscellaneous : -