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

MASTER THESIS PROPOSAL

Dates: April 2020 - September 2021

Laboratory: Quantum Information Theory
Institution: ICFO
City, Country: Castelldefels, Spain

Title of the master thesis: Bound entangled states in device-independent quantum key distribution

Name of the master thesis supervisor and co-supervisor: Antonio Acín, Máté Farkas
Email address: mate.farkas@icfo.eu, antonio.acin@icfo.eu

Keywords: bound entangled states, device-independent quantum key distribution

Summary of the subject:

Entanglement is a counter-intuitive feature of particles in quantum theory, predicting that experimental observations on distant particles can be correlated in a manner that is inexplicable in classical physics, i.e., under the assumption of **local realism**. In other words, if we assume that particles have pre-determined properties defined locally (at the position of the particle), we will arrive at contradictions with the predictions of quantum theory. This contradiction was first pointed out by Einstein, Podolsky and Rosen [1], and later formalised by Bell [2], via the so-called "Bell inequalities". Bell inequalities bound linear combinations of outcome probabilities of measurements performed by distant parties, and are satisfied in any local realist theory. However, these inequalities can be violated in quantum theory, in particular, by using quantum states that are entangled between the distant parties. Remarkably, the violation of Bell inequalities has recently been confirmed in so-called "loophole-free Bell tests" [3-5], ruling out local realist models of nature.

The violation of Bell inequalities turns out to be a useful resource beyond its fundamental implications. As a prominent example, certain Bell inequality violations allow for the generation of a secure cryptographic key between the distant parties. Importantly, to prove security, the parties do not need to assume anything about the inner workings of their devices, apart from the correctness of quantum theory and the space-like separation of their measurements. The cryptographic security of the key is simply deduced from the observed Bell inequality violation under these assumptions, and therefore such cryptographic protocols are referred to as **device-independent quantum key distribution** (DIQKD) [6].

Known secure DIQKD protocols usually employ states that are strongly entangled (often the so-called “maximally entangled state”). These states are naturally the most promising candidates for DIQKD, however, little is known about the general structure of useful entangled states for DIQKD. In particular, arguably the weakest class of entangled states that might still be useful for DIQKD is that of **bound entangled states** [7]. Bound entangled states are entangled states from which it is impossible to “distill” a maximally entangled state by local operations and classical communication, even if there are arbitrarily many copies of the state available. It has been famously conjectured by Peres that bound entangled states cannot be used to violate any Bell inequality [8], but 15 years later Vértesi and Brunner found a bound entangled state violating a specific Bell inequality [9]. Recently, Arnon-Friedman and Leditzky introduced a “revised Peres’ conjecture”, stating that bound entangled states cannot be used for DIQKD [10], however, this conjecture is based on the single construction by Vértesi and Brunner.

Since the seminal paper of Vértesi and Brunner, many families of bound entangled states have been found that violate Bell inequalities [11-12]. In this project, we will study these known families in the context of DIQKD in order to gain more evidence for, or disprove the “revised Peres’ conjecture”. In particular, we will compute lower bounds for DIQKD key rates, by computing the Devetak–Winter rate [13] using semidefinite programming techniques [14]. Furthermore, we will also compute upper bounds on the key rates, by computing the intrinsic information for specific eavesdropping attacks, using linear programming techniques [15]. Apart from tackling the “revised Peres’ conjecture”, this work will advance the characterisation of resources useful for DIQKD.

References:

[1] A. Einstein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777 (1935)
[2] J. S. Bell, Physics **1**, 3 (1964)
[3] Hensen et al., Nature **526** (2015)
[4] Giustina et al., Phys. Rev. Lett. **115**, 250401 (2015)
[5] Shalm et al., Phys. Rev. Lett. **115**, 250402 (2015)
[6] A. Acín et al., Phys. Rev. Lett. **98**, 230501 (2007)
[7] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998)
[8] A. Peres, Found. Phys. **29**, 589–614 (1999)
[9] T. Vértesi, N. Brunner, Nat. Comm. **5**, 5297 (2014)
[10] R. Arnon-Friedman, F. Leditzky, arXiv:2005.12325 (2020)
[11] S. Yu, C. H. Oh, Phys. Rev. A **95**, 032111 (2017)
[12] K. Pál, T. Vértesi, Phys. Rev. A **96**, 022123 (2017)
[13] I. Devetak, A. Winter, Proc. R. Soc. Lond. A, **461**, 207–235 (2005)
[14] E. Y.-Z. Tan et al., arXiv:1908.11372 (2019)
[15] A. Acín, S. Massar, S. Pironio, New J. Phys. **8**, 126 (2006)

Additional information:
* Required skills: Knowledge of linear algebra and quantum formalism, basics of coding