Gdańsk, 28th of June, 2018

mgr Edgar Alexis Aguilar Lozano
Institute of Theoretical Physics and Astrophysics
University of Gdansk

ABSTRACT OF DOCTORAL DISSERTATION

Device Independent and Semi Device Independent Protocols for Quantum Information Processing

The doctoral dissertation examines different device independent (DI) and semi device independent (SDI) protocols and their applications to quantum information processing. A remarkable feature of device independent protocols is that the parties involved need not make any assumptions about the inner workings of their devices. In particular they do not need to trust the source that produces the systems which the parties measure nor the measurement apparatuses. This scenario is ideal for cryptographic tasks, where two parties that want to establish a secret key do not trust the supplier of their experimental devices or they have reason to believe there is an eavesdropper on the quantum channel. In a similar fashion, semi device independent protocols make almost no assumptions on the devices either, except for limiting the dimension of the physical systems used (or equally, by limiting the channel capacity). The SDI approach is less strict (thus, less secure), but it is extremely valuable for testing experimental capabilities in the prepare-and-measure scenario. Due to very limited assumptions that are made, unprecedented levels of security can be obtained, which explains the amount of both experimental and theoretical research that is being carried out. This dissertation is theoretical in essence, although part of the work was designed to be experimentally implemented (which it was, successfully).

In particular, a collection of device independent protocols that are useful for randomness expansion were used alongside well-established DI-quantum key distribution protocols in order to challenge the underlying assumptions that are needed to guarantee privacy. The necessity of having access to a random number generator is questioned, since these devices do not fulfill the DI condition, and a protocol that can establish a secret key between two parties in a completely device independent way is given.

Finally, a semi-device independent protocol known as Random Access Codes (RACs) is analyzed and a couple of applications are found. One application is meant to provide a statistical test to certify high dimensional quantum states in an experiment. This was implemented in a photonic experiment and a 1024 dimensional state was certified. The other application provides an explicit algorithm to rule out the existence of a given number of mutually unbiased bases in a particular dimension.