UNIWERSYTET MIKOŁAJA KOPERNIKA

INSTYTUT FIZYKI

ul. Grudziądzka 5/7 87-100 TORUŃ
http://www.fizyka.umk.pl/
Tel. centr. (48 56) 611 33 10 Fax (48 56) 622 53 97
Sekretariat: (48 56) 622 63 70 e-mail: ifiz@fizyka.umk.pl

Toruń, September 3, 2018

prof. Dariusz Chruściński
Institute of Physics
Nicolaus Copernicus University
Torun, Poland

Report on the PhD Thesis by Edgar Alexis Aguilar Lozano

„Device Independent and Semi Device Independent Protocols for Quantum Information Processing"

The presented thesis is devoted to the analysis of certain quantum information protocols which possesses an extra property being device or semi device independent (DI and SDI, respectively). Quantum information is one of the pillars of modern quantum theory which not only proves the theoretical supremacy of quantum protocols over classical ones but also found fundamental practical applications. It is, therefore, clear that the topic of the PhD thesis belongs to the important and active area of research.

The thesis consists of three papers published in leading journals in the field:

1. E. A. Aguilar, R. Ramanathan, J. Koer, M. Pawłowski, *Completely device-independent quantum key distribution,* Phys. Rev. A **94**, 022305 (2016).
2. E. A. Aguilar, M. Farkas, D. Martinez, M. Alvarado, J. Carine, G. B. Xavier, J. F. Barra, G. Canas, M. Pawłowski, G. Lima, *Certifying an irreducible 1024-dimensional photonic state using refined dimension witnesses,* Phys. Rev. Lett. **120**, 230503
3. E. A. Aguilar, J. J. Borka la, P. Mironowicz, M. Pawłowski, *Connections Between Mutually Unbiased Bases and Quantum Random Access Codes*, Phys. Rev. Lett. **121**, 050501 (2018)

supplemented by the Summary of PhD Dissertation (16 pages). All three papers are multi-author and the PhD documentation contains declarations of all coauthors about their contributions.

Paper 1: (4 authors) contribution of the Autor 65%
Paper 2: (10 authors) contribution of the Autor 30%
Paper 3: (4 authors) contribution of the Autor 50%

Edgar Aguilar is also a coauthor of the paper

J. K. Korbicz, E. A. Aguilar, P. Ćwikliński, P. Horodecki, *Generic appearance of objective results in quantum measurements*, Phys. Rev. A **96**, 032124

and his contribution is 35%. It certifies that Edgar Aguilar is a key author for all three presented papers.

Paper 1 is devoted to new schemes of quantum cryptography. A key issue for any cryptographic protocol is security which for the entanglement based quantum key distribution (QKD) relies upon the violation of certain Bell inequalities. Few years ago it has been shown that such protocols may be realized in a device-independent way - DIQKD, that is, two parties involved in QKD need not make any assumption about the devices they use. In particular it applies to the sources producing entangled pairs used in the protocol and measurement apparatuses used by the parties. However, to run the protocol the parties have to use certain source of randomness and the weak point is that there is no fully trusted random number generators which could provide such perfect source of randomness. Hence on the one side the parties do not need to trust the device but they have to trust the source of randomness which is never perfect. The big achievement of the Author is the proposal of the new protocol called completely DIQKD (CDIQKD) in which there is no need to trust the devices nor the random generator.

The CDIQKD protocol is based on four assumptions: 1) no-signaling condition is imposed on the devices, 2) the parties use authenticated classical communication channel (needs not be secure), 3) the protocol is fully based on quantum mechanics (no super-quantum correlations are allowed), 4) one party (say Alice) possesses a message sufficiently random with respect to the potential eavesdropper (Eve) and the devices (it is measured by sufficiently large min entropy). Then using the protocol of randomness expansion the Author proved the security of CDIQKD.

This is very elegant result which can influence the field of quantum cryptography substantially. One may wonder is it still possible to relax part of the assumptions used in the proof of security.

Paper 2 and 3 discusses applications of SDI protocols which are less demanding that DI ones. In particular SDI protocol usually makes some additional assumptions about the dimensionality of the quantum system (Hilbert space). Clearly, they are more accessible for implementation. Essentially, any DI protocol has an SDI analog which is easier to implement in the laboratory. In the thesis Author concentrates on a particular protocol so called random access code (RAC) and its quantum counterpart (QRAC). In paper 2. these protocols are used for the construction of the new class of dimension witness. The new feature of these witnesses is that they have different bounds for all possible decompositions of the total Hilbert space of the system which can be represented (decomposed) as a tensor product of lower dimensional Hilbert spaces. This is very interesting aspect of the witness which can be used to certify whether the system living in the high dimensional Hilbert space is decomposable into lower dimensional subsystems. This aspect is completely new with respect to dimension witnesses used so far in the literature. Such witness was successfully used in paper 2. to certify the irreducibility of 1024-dimensional photonic state.

Another very interesting application of RAC and QRAC is reported in Paper 3. The Author introduces a new protocol - so called promise-Quantum Random Access Code (pQRC) - and uses it for the construction of a new measure of unbiasedness for bases in the Hilbert space. Such measures were already proposed in the past (e.g. the measure of Bengtsson and Życzkowski). However, the measure proposed by the Author has clear operational interpretation which was not the case for the previous measures. The power of the protocol comes from the fact that employing semi-definite programming it may be used to investigate whether a specific number of mutually unbiased bases (MUBs) exists for a given dimension of the Hilbert space. This problem is highly nontrivial since for a given dimension d we know only an upper bound N=d+1 of MUBs. Moreover, it was shown that if d is a power of prime then there are exactly d+1 MUBs. The first problematic case is d=6 and it is not known whether there exists more than 3 MUBs. Using the pQRC the Author shown that there is no 5 MUBs for d=3, and excluded the existence of 6 MUBs for d=4. Unfortunately, the protocol still failed to ruled out the existence of 4 MUBs for d=6.

The final conclusion: in my opinion the PhD thesis of Edgar Alexis Aguilar Lozano provides an important contribution in the field of quantum information (particularly in quantum processing and quantum complexity). The thesis contains essential developments of new methods and provides new important and very interesting results. It should be stressed that all results were already published in a series of articles in Phys. Rev. Lett. (two papers) and Phys. Rev. A (one paper) and hence they were already reviewed (each paper published in Phys. Rev. Lett. has at least two referees) and accepted by the experts in the field. **I have no doubt that Edgar Alexis Aguilar Lozano fully deserves PhD in physics. Moreover, in my opinion considered PhD thesis should be accepted with honours.**

D. Chruściński
Dariusz Chruściński