Annex 7: Habilitation thesis reviewer's report

Masaryk University
Faculty of Informatics
Habilitation field: informatics

Applicant: RNDr. Jan Bouda, Ph. D.
Unit: Faculty of Informatics Masaryk University, Brno
Habilitation Thesis: Randomness in (Quantum) Information processing

Reviewer: Prof. Marek Żukowski
Unit: Institute for Theoretical Physics and Astrophysics, University of Gdansk, Poland.

Reviewer's report

As my first remark I would like to state that the overall input to science by dr Bouda is pointing to the fact that he might deserve the degree of doctor habilitatus, still this is a qualification right at reaching the threshold in size, importance and other characteristics of full overall scientific output, without any "spare volume". Still this view of mine can be biased by the standards usual to physics, whereas the candidate is a specialist in computer science. Nevertheless, his work is on physical aspects of information processing, in the context of the new opportunities given by our current, and future, control of quantum systems which can used to construct new devices for such tasks. Most of the papers were published in physical journals, thus my bias might be justified: if one treats the contributions as centered in quantum information, which is a part of physics, alas much linked with information and computer science, the overall size and importance of his contribution to this field is quite low, especially as he is now 11 years after his Ph.D. Still the bibliographic parameters could look perhaps good enough for this stage of his career. According to Web of Science the Candidate published 15 papers, which were cited thus far 176 times. This looks quite impressive, however the bulk of the citations, 125, are of a collaborative paper on cryptographic network experimental presentation in Vienna, with around 50 co-authors or more... If one deduces this number, the actual citations of works, in case of which dr Bouda had a significant impact on their form and content, drops to 51 times, which is not that impressive. The most cited paper thus far, 19 citations, concerns multi-qudit entanglement swapping, a kind of generalization of our ideas of 1993. All this gives rather a borderline case, again pointing to the fact that the Habilitation Thesis is carved out of set of papers which is perhaps just enough to get it, but nothing more. Additionally, one must say that the Candidate did not publish any paper this year, neither there is any entry of his authorship to arXiv.org/quant-ph in 2015. This is strange as the field of quantum information is developing at a break-neck speed with way over 100 new manuscripts appearing in arXiv per week. The last entry of dr Bouda

to the Internet-repository is from February 2014... Still, the Candidate boasts an impressive number of conference talks, has received some grants, and was a member of committees of various conferences, and has an extensive didactic experience in teaching classical computer science (with one series of lectures or classes on quantum information).

Concerning the Thesis, before I shall state my opinion on its scientific content, I must reveal my formal doubts. Two of the papers of the collection which forms the thesis, namely [4] and [5], were published in 2003, that is before dr Bouda received his Ph.D. As I know nothing about the contents of the Ph. D Thesis, I think the local commission should check whether these works were or were not a part of the Ph. D. Thesis. Still the title of the Pd. D. Thesis is "Encryption of Quantum Information and quantum Cryptographic Protocols" while the title of the work [4] is "Encryption of Quantum information", which exactly matches the first part of the title of the thesis, whereas the title of [5] is "Security of the private quantum channel", that is, it is about quantum cryptographic protocols. According to Polish academic standards, works which were published before awarding the doctoral degree, cannot form a part of paper collection treated as a Habilitation Thesis. If the customs in the Czech Republic are different, then these remarks of mine should be counted as irrelevant.

The other reservation that I have is that the collection contains papers which have basically the same content. E.g., [12] seems to be just a conference version of [13], and I see no significant difference between the two papers. Also, I do not see basic difference between papers [4] and [5], additionally the first part of [9] has a significant overlap with these. One more strange thing: the papers in the collection are numbered 2, 4-7 and 9-16, with 1, 3 and 8 missing... This is pretty confusing.

The collection of papers in general studies the question of encryption of quantum information (this a different problem than the usual quantum cryptography, in the case of which the secret is classical), randomness amplification, and randomness generation. With the exception of works [10, 15], all this is in the context of quantum information methods. Paper [10] suggests that one might use internal source of noise in cellular phones to harvest random sequences. As I am not a specialist in modern communication technologies, it is difficult for me to judge whether the approach of [10] is novel, and practical.

The works which address the quantum information protocols seem to be fully in concurrence with the title of the Thesis "Randomness in (Quantum) Information Processing". While the results contained in the Thesis see correct, and have some degree of originality, their impact on the current literature is low. Only the work [7] "Weak randomness seriously limits the security of quantum key distribution" seems to be affecting research of other scientists.

The works [4,5,9] address interesting aspects of quantum private channels (that is methods to securely transfer quantum information). There is a paradoxical difference between such protocols with classical or quantum cryptography. In the latter possession many copies of the cipher-text is of no value for the eavesdropper, while surprisingly this may be a problem for private quantum channels. The Authors of the papers address attacks on private quantum chan-

nels utilizing partial knowledge of the classical description of the cipher-text. In [9] a generalization of the results to approximate encryption is made. Of course, once more I have to express by doubts whether the works [4,5] can be counted as a contribution to the Habilitation Thesis, as their content seems to be a recycling of part of the material for the Doctoral Thesis (I may wrong here, but all points to this...).

The work [11] studies the problem of private quantum channels, and possible occurrence of multi-photon pulses. Note here that in the case of the workhorse phenomenon of experimental quantum information, that is for parametric down conversion, such events may indeed happen if the pumping is too strong. In case of such instances the standard security analysis cannot be applied. The authors prove that if the states which are to be transferred are proper mixed states, there is no secure method of encryption. However, for pure states there is no problem and the optimal encrypting scheme for k-photon pulse is equivalent to the so-called unitary k-design. By the way, passive optical devices would give us this for free, provided we use the 1-design encryption for single photons, but this is my side remark. Still I put it here, to show that the proposed scheme while it seems contrived, in fact is quite feasible.

The question of optimal encryption in private quantum channels is addressed in [16]. The entropy exchange function is studied, which quantify the amount of information lost to the external system, imposing the random unitaries, which provides the encryption. This is given by the Von Neumann entropy of the external system (which the authors call, somehow misleadingly, environment). This in turn is shown to provide the lower bound for the entropy of the classical key needed for the encryption (and the decryption by the receiver). Special cases of all that are discussed.

The work [2] studies an additional requirement for a good quantum encryption protocol: one must be sure that an adversary cannot affect the "plain-text" (that is the encrypted states) in a predictable way. It is shown that quantum private channels having this property (non-malleability) are equivalent to unitary 2-designs. In their case the only predictable action possible for the adversary is addition of "white noise", and thus it is just a partial destruction of the channel, rather than taking over the control. The study is extended to various non-perfect situations, and some generalizations are given in [6].

The next set of works is addressing various security aspects of quantum cryptography, with imperfect sources of randomness. In [7] it is shown that an imperfect "weak" randomness, used to select check positions in the test of security of quantum key distribution, can kill the whole security of the protocol. On the positive side in [14] the Authors show that, while In classical cryptography unconditional security is impossible for schemes which use "weak" randomness to generate keys, with quantum cipher-texts the potential adversary's probability to guess correctly the plain-text dives under bound for classical encryption schemes.

Papers [12,13, 15] address randomness extraction. Works [12,13], as it was said above, are basically identical in their results. [12] is simply a shorter version of [13], with most appendices dropped. It suggests use of a quantum protocol for

randomness extraction, which is "device independent". That is its properties can be checked by the users without any knowledge about the actual workings of the devices. The authors use a scheme which employs the Greenberger-Horne-Zeilinger correlations, and the Mermin-Bell inequalities. I think the work [14] may in future gain quite a lot of citations. In [15] the randomness extractor uses a Hadamard matrix approach. The protocol is classical, thus I am not entitled to judge it.

In summary the Thesis effectively consists of original 11 works, out of which 10 were published after the Candidate had been awarded his doctoral degree. I do not understand why some of the works in the selection contain basically the same material. Also, I cannot understand why they are put in an, indeed, random sequence. They are neither grouped thematically, not put in a monotonic temporal sequence of dates of publication. Is this a "selection" at all? Thus far, the works gained very little attention of scientists working in the field. Still I find the results of [2,11,13,16] quite interesting, and thus my final opinion on the Thesis in (weakly) positive.

Reviewer's questions for the habilitation thesis defence

1. Why the Thesis contains works which had been published before the Candidate was awarded Ph. D.? Why almost identical papers are included in the Thesis? Why the papers of the thesis are not grouped thematically of chronologically?

2. Please explain the concept of device independent protocols and "Mermin devices". What are the basic difficulties in experimental realizations of device independent protocols?

Conclusion

The habilitation thesis submitted by Jan Bouda entitled *Randomness in (Quantum) Information Processing* meets the requirements applicable to habilitation theses in the field of informatics.

In Gdansk on 01.10.2015