

## **Annex 6: Habilitation thesis reader's report**

**Masaryk University**

**Faculty** MU Faculty of Informatics

**Field of Habilitation** Informatics

**Applicant** Mgr. Mário Ziman, Ph.D.

**Affiliation** Masaryk University, Faculty of Informatics

**Habilitation Thesis** Quantum encryption protocols and programmable processors

**Reader** Prof. Dr. Caslav Brukner

**Affiliation** Universität Wien

### **Report Text (as large as the reader deems necessary)**

The habilitation thesis of Dr. Mario Ziman, entitled “Quantum encryption protocols and programmable processors” considers – as the title of the thesis suggest – various ways of and differences between classical and quantum encryption as well as programmable quantum processors. After brief introduction into the basic concepts of quantum information in the chapter “Elements of quantum information theory” the thesis presents original work divided into two further chapters, “Quantum protocols” and “Programmable quantum processors”. Each chapter is accompanied with a short introduction into the topic followed by attached reprints of publications relevant for the topic.

The work that is reported in the thesis has been published in 10 articles in collaboration with various researchers, among others with Prof. Vladimír Buzek and Prof. Mark Hillary, who are among the leading scientists in the field of quantum information. The articles are published in reputable journals including Physical Review A and Journal of Physics A.

In the first chapter Dr. Ziman gave a succinct overview of quantum information theory basics. The most necessary mathematical and information-theoretical concepts were introduced for understanding the research results presented in the subsequent chapters.

The second chapter mainly concerns with quantum dense coding as one of the most remarkable demonstrations of how entanglement can be used as a resource in coding. One of the most interesting problems addressed there is the analysis of how the capacity of single-qubit channel depends on the correlations shared by separated partners. In a joint work with Prof. Buzek, Dr Ziman gave a set of local unitary transformations that generate out of a partially entangled state of the qubits four maximally distinguished states of the two qubits. The results were generalized to higher-dimensional systems as well. Still within the same chapter is the work of potential wide application on a new scheme for quantum-based privacy and voting.

A significant portion of the work is devoted to programmable quantum processors. It is presented in the third chapter of the thesis and has resulted in 6 publications of which five in Physical Review A. A programmable quantum processor is a quantum circuit in which both the data and the program that specifies the operation on the input are quantum states. One of the most interesting results from this research direction is the proof of impossibility of designing a finite processor for the amplitude-damping channel, though such a processor is

possible for the phase damping-channel. Another result addresses the probability of success in the probabilistic implementation of universal quantum processors. It was shown that, while this probability scales as inverse of square of Hilbert dimension, the scaling can be improved for restricted sets of operators or by using the processors in loops. More relevant from the practical point of view are approximate quantum processors that approximate a set of unitary operators to a specific level of precision that might be sufficient for real measurements which are always of limited precision.

The thesis presents a collection of original, sound, and interesting research results that tackles some open problems in theoretical quantum information. It is worth reminding of the author's capability of finding rigorous mathematical proofs for the problems posed. The thesis is written in a concise but accurate way. Particularly relevant for the Faculty of Informatics is that Dr. Ziman work's is at the cutting edge science positioned between information theory and quantum physics. Until recently the common notion of computing was based on the laws of classical physics. Yet, in last two decades it was realized that harnessing quantum mechanical laws for information processing allows accomplishing computational and communicational tasks that are classically impossible. A modern scientific and educational institution in informatics should not miss an opportunity to get such a high-quality specialist in quantum information.

I have no doubts that Dr Ziman will be great enrichment for the Faculty of Informatics, at the Masaryk University.

In conclusion, I evaluate the thesis with "excellent".

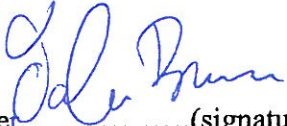
**Reader's questions to answer to defend the habilitation thesis (number of questions is upon reader's consideration)**

1. What do you think will be the final output of quantum information science?
2. Imagine that you have ability to manipulate 100 qubits coherently. What would you use them for? Give arguments that no device based on classical laws and on comparable number of bits cannot do the same.

**Conclusion**

Mário Ziman's habilitation thesis of "Quantum encryption protocols and programmable processors" *does* meet the standard requirements for a habilitation thesis in the field of Informatics.

In Vienna on 07.10.2010.....

  
Caslav Brukner .....(signature)