Příloha 6: Posudek oponenta habilitační práce

Masarykova univerzita	
Fakulta	Fakulta informatiky MU
Habilitační obor	Informatika
Uchazeč	Mgr. Mário Ziman, Ph.D.
Pracoviště	Fakulta informatiky, Masarykova univerzita
Habilitační práce	Quantum encryption protocols and programmable processors
Oponent	Prof. RNDr. Miloslav Dušek, Dr.
Pracoviště	Univerzita Palackého v Olomouci – Přírodovědecká fakulta

Text posudku (rozsah dle zvážení oponenta)

The habilitation thesis deals with a new and rapidly developing area of information science which exploits the power of quantum physics. It represents a brief overview of several families of quantum information protocols and contains ten selected original papers from the same field. In particular, the author discusses quantum information encryption (including quantum dense coding and quantum teleportation), quantum privacy, and quantum-programmable quantum processors and measurement devices. The first chapter after the Prologue represents a concise review of the elements of quantum information theory and related mathematical tools. Each of the next two chapters consists of introductory texts and collections of the copies of related papers. The introductory parts are clearly written and they document author's pedagogical skills. They provide the reader with prerequisites necessary for reading subsequent author's papers. However, in some cases they are perhaps too compact. The enclosed publications approve author's high scientific erudition and creativity. They are from years 2000-2007. In four of these ten papers Mario Ziman is the first author. All of the works have brought original contributions to the field and have been published in prestigious journals (seven of them in Physical Review A).

Mario Ziman is a recognized expert in the field of quantum information theory (H index 10, 40 papers at WOS, over 290 citations). The submitted habilitation thesis confirms both his scientific and pedagogical qualities.

Dotazy oponenta k obhajobě habilitační práce (počet dotazů dle zvážení oponenta)

1. In the abstract the author writes "Quantum NOT isn't a physically feasible transformation but we can build a gate implementing the square root of logical operation NOT." There is a couple of quantum NOT gates: A universal NOT, a "logical" NOT, an approximate universal NOT, and a controlled NOT. Could the author clarify the differences between these gates and explain which of these NOT gates he meant in his sentence?

2. In Sec. 4.2 it is mentioned that in the case of probabilistic programmable quantum devices the encoding of unitary operations by means of quantum states of the program register is qualitatively different from the encoding of quantum measurements. Is there any intuitive physical explanation for this difference?

Závěr

Habilitační práce Mária Zimana „Quantum encryption protocols and programmable processors“ ***splňuje*** požadavky standardně kladené na habilitační práce v oboru Informatika.

Olomouc, 25. června 2010

Miloslav Dušek .....