Příloha 7: Posudek oponenta habilitační práce

Masarykova univerzita	
Fakulta	Fakulta informatiky MU
Habilitační obor	Informatika
Uchazeč	RNDr. Jan Bouda, Ph.D.
Pracoviště	Fakulta informatiky Masarykovy univerzity
Habilitační práce	Randomness in (Quantum) Information Processing
Oponent	doc. Mgr. Jaromír Fiurášek, Ph.D.
Pracoviště	Katedra optiky, Univerzita Palackého v Olomouci, Olomouc

Text posudku

V předložené habilitační práci se Dr. Jan Bouda věnuje problematice náhodnosti v kvantovém zpracování informace. Jedná se o velmi důležitou a aktuální tématiku a habilitační práce obsahuje řadu původních autorových výsledků dosažených v této oblasti. Habilitační práce má podobu komentovaného souboru vědeckých prací a je psána anglicky. Jak úvodní komentář, tak i jednotlivé přiložené vědecké práce jsou kvalitně zpracované jak po odborné, tak i po jazykové stránce, text je jasný, srozumitelný a vhodně strukturovaný.

V první kapitole úvodního komentáře autor nastiňuje motivaci pro studium náhodnosti v kvantovém zpracování informace a stručně specifikuje tematické zaměření habilitační práce. Následně ve druhé kapitole autor detailněji popisuje jednotlivé oblasti výzkumu, na něž je habilitační práce zaměřená, a shrnuje hlavní výsledky a stav poznání, které tvořily východisko pro autorův vlastní výzkum v těchto oblastech. Následně ve třetí kapitole autor shrnuje své výsledky dosažené v následujících třech souvisejících oblastech výzkumu: náhodnost v šifrování a unitární k-designy, slabá náhodnost v kryptografických aplikacích a extrakce náhodnosti. Úvodní komentář je doplněný o seznam literatury a přehled vědeckých prací, které tvoří jádro habilitační práce.

Mezi nejvýznamnější autorovy výsledky v oblasti náhodnosti v kvantovém šifrování patří například návrh privátního kvantového kanálu, který nejenže neumožňuje tomu, kdo tajně odposlouchává, získat žádnou informaci o kvantovém stavu posílaném od odesilatele příjemci, ale zároveň také výrazně limituje možnost neoprávněné manipulace se zašifrovaným kvantovým stavem. Ukazuje se, že takovýto privátní kvantový kanál lze vytvořit pomocí náhodně volených unitárních operací, které tvoří tzv. unitární 2-design. Autor dále poukázal na nový typ kryptografického útoku na privátní kvantové kanály, který je založený na znalosti zašifrovaného kvantového stavu. Autor rovněž detailně studoval efektivitu šifrovacích strategií měřenou počtem bitů klasického klíče, které jsou potřeba na přenos jednoho zašifrovaného kvantového bitu.

V další části práce se autor zaměřil na problematiku slabé náhodnosti a poukázal na to, že slabá náhodnost může výrazně ovlivnit a snížit bezpečnost kvantově kryptografických protokolů. Autor se specificky zaměřil na případ, kdy slabě náhodné klasické bity jsou použité

v protokolu BB84 k volbě pozic kvantových bitů, které slouží k charakterizaci šumu v kvantovém kanálu mezi Alicí a Bobem. Bylo ukázáno, že libovolná slabá náhodnost postačuje k tomu, aby tento protokol přestal být bezpečný, pokud se pro charakterizaci kvantového kanálu použije pouze sub-lineární část z celkového počtu bitů hrubého klíče (raw key). Autor dále navrhl šifrovací systém, který kóduje klasickou zprávu do kvantového stavu pomocí klasického klíče. Ukazuje se, že tímto postupem je možné překonat tzv. McInnes-Pinkasovu mez na pravděpodobnost, že zpráva bude odhalena protivníkem.

Ve třetí části práce se autor zaměřuje na extrakci náhodnosti ze zdrojů slabé náhodnosti. Autor například navrhl přístrojově nezávislý extraktor náhodnosti, který využívá tzv. Merminova zařízení. Tento postup je metodologicky analogický k přístrojově nezávislé kvantové kryptografii, kde bezpečnost generovaného klíče je garantována pozorováním porušení Bellových nerovností bez ohledu na interní konstrukci přístrojů použitých Alicí a Bobem při Bellově testu. Autor rovněž navrhl metodu generace vysoce kvalitní náhodnosti pro kryptografické účely pomocí mobilních zařízení, zejména mobilních telefonů.

Jednotlivé publikace tvořící jádro habilitační práce vznikly ve spolupráci autora s domácími i zahraničními kolegy, což svědčí o autorově schopnosti úspěšně se zapojit do vědecké spolupráce na mezinárodní úrovni. Současně je však jasně patrný a doložený výrazný podíl Dr. Jana Boudy na jednotlivých publikacích. Významná část publikací tvořících jádro habilitační práce byla publikována v mezinárodních impaktovaných časopisech, což potvrzuje vysokou odbornou úroveň habilitační práce. Závěrem mohu konstatovat, že se jedná o velmi zdařilou a kvalitní práci, která přináší řadu důležitých původních vědeckých výsledků v oblasti náhodnosti v kvantovém zpracování informace.

Dotazy oponenta k obhajobě habilitační práce

1. V práci Ref. [7] je ukázáno, že slabá náhodnost vede k tomu, že protokol BB84 pro kvantovou kryptografii neumožňuje generovat žádný bezpečný klíč. Jako možné řešení tohoto problému je zmíněno použití významné lineární části bitů hrubého klíče pro charakterizaci kvantového kanálu, což ovšem vede k redukci délky generovaného klíče. Bude platit, že délka generovaného bezpečného klíče bude v tomto případě přímo úměrná celkovému počtu kvantových bitů přenesených od Alice k Bobovi? Pokud ano, v jakých případech by autorem zmiňovaná redukce délky generovaného tajného klíče mohla představovat významný problém?

2. V publikaci Ref. [6] je uvedeno, že multidimenzionální integrály, které se vyskytly v prováděných výpočtech, bylo velmi obtížné vypočítat analyticky i numericky s použitím standardních kvadraturních metod. Mohl by autor objasnit, v čem spočívala náročnost těchto výpočtů a proč nešlo využít např. Schurova lemmatu?

3. V práci Ref. [11] autor uvažuje vstupní k-fotonové stavy, které jsou matematicky popsané maticí hustoty, která je tenzorovým součinem k matic hustoty kvantových stavů jednotlivých fotonů. To odpovídá situaci, kdy uvažované fotony jsou vzájemně rozlišitelné, i když připravené v identických (smíšených) stavech. Naproti tomu, pokud by se jednalo o nerozlišitelné fotony, což může být například případ slabých koherentních laserových pulzů, pak by matice hustoty výsledného k-fotonového (smíšeného) stavu náležela do třídy operátorů působících na symetrickém podprostoru

k qubitů. Obecně by pak bylo možné uvažovat částečně rozlišitelné fotony. Jaký vliv by měla případná částečná či úplná nerozlišitelnost fotonů na výsledky uvedené v Ref. [11]?

Závěr

Habilitační práce Jana Boudy „*Randomness in (Quantum) Information Processing*“ ***splňuje*** požadavky standardně kladené na habilitační práce v oboru Informatika.

Olomouc, dne 31. 8. 2015

doc. Mgr. Jaromír Fiurášek, Ph.D.

UNIVERZITA PALACKÉHO V OLOMOUCI
PŘÍRODOVĚDECKÁ FAKULTA
KATEDRA OPTIKY
tř. 17. listopadu 12, 771 46 Olomouc