Oponentský posudek na diplomovou práci pana Ondřeje Čermáka

Quantum cryptography with time and phase encoding

Práce se zabývá simulací a modelovou experimentální implementací zařízení pro kvantový přenos klíče pomocí protokolu BB84 s využitím fázového kódování. Práce je psána anglicky na dobré jazykové úrovni. Včetně úvodu a závěru sestává celkem ze sedmi kapitol a čítá 116 stran. V kapitole druhé jsou představeny a vysvětleny potřebné teoretické metody a matematické nástroje, konkrétně základní pojmy kvantové mechaniky a teorie informace. Třetí kapitola zahrnuje stručný úvod do kvantové kryptografie a rešerši několika vybraných protokolů pro kvantovou distribuci klíče, v jejím závěru jsou popsány klasické algoritmy potřebné pro realizaci kvantové distribuce klíče. Čtvrtá kapitola se zabývá otázkami bezpečnosti kvantové distribuce klíče, mimo jiné je zde popsáno několik vybraných typů útoků. Vlastní výsledky autora jsou prezentovány zejména v kapitolách pět a šest. Kapitola pět popisuje stručně procedury pro simulaci kvantové distribuce klíče s využitím protokolu BB84, fázového kódování a metody „decoy states". Jsou zde také prezentovány výsledky simulací pro různé hodnoty ztrát a různé typy a hodnoty započteného šumu. V kapitole šest je představeno zjednodušené experimentální uspořádání pro výše uvedený typ protokolu a kódování. Jsou zde popsány použité optické a elektronické komponenty, jakož i konstrukce a testování zařízení. Experiment však nebyl dotažen do konce, přenos klíče demonstrován nebyl. Text je doplněn seznamem použité literatury, který obsahuje 63 položek.

Vlastní autorova práce spočívá ve vytvoření programového vybavení pro simulaci kvantové distribuce klíče a v částečné realizaci laboratorního uspořádání pro demonstraci kvantové distribuce klíče. Z práce lze usuzovat, že autor prokázal dostatečné porozumění teoretickým základům studované problematiky i potřebnou experimentální zručnost.

Poznámky k formální podobě práce:

- Zdá se, že student chtěl v práci alespoň stručně zmínit vše, s čím se setkal při studiu literatury, i když to s tématem práce souviselo jen nepřímo nebo vůbec (např. výpočet dvojitého interferometru z obr. 3.3). To ale kvalitu práce nezvyšuje, spíše ji to činí méně přehlednou a hůře čitelnou.
- V několika případech se výklad opakuje na více místech textu v podobném rozsahu a formě (např. *intercept-resend attack* na str. 44 a 69). Na několika místech se dokonce opakují celé odstavce těsně za sebou. Jsou sice napsány různými slovy, ale mají stejnou strukturu a obsahují zcela stejné informace (např. dva odstavce na str. 2, dva odstavce na str. 41, nebo dva odstavce na str. 47).
- Některé věty jsou pravděpodobně jen neodstraněnými interními poznámkami autora (např. 3. odstavec na str. 69).
- V práci se také objevuje několik odkazů na vzorce směrem dopředu (do textu, který teprve následuje). To čtení práce neusnadňuje.
- Některá vyjádření jsou nepřesná, např. na str. 3 se píše „... bipartite systems of two quantum states ...". Systém se neskládá ze stavů, systém je v nějakém stavu. Podobně na str. 6, systém se neskládá z Hilbertových prostorů, Hilbertovy prostory slouží pro popis stavu systému.

Poznámky k obsahu práce:

- V abstraktu jsou uváděny hodnoty interferenčního kontrastu, aniž by bylo řečeno v jakém uspořádání, za jakých podmínek a jak byly měřeny. Bez zmíněného kontextu jsou to čísla, která čtenáři nedávají žádnou užitečnou informaci.
- V rov. (2.6) na str. 7, se míchá dohromady matice a bra-vektor (tedy funkcionál na $\mathcal{H}_B$), resp. ket-vektor (vektor z $\mathcal{H}_B$). Výraz dává dobrý smysl bez $\mathbb{I}$ (ρ_A je operátor působící na $\mathcal{H}_A$).
- Definice superoperátoru na str. 8 jsou trochu zmatečné. Jako superoperátor se obvykle označuje zobrazení z prostoru operátorů (matic hustoty) do prostoru operátorů bez ohledu na dimenzi.
- Na str. 9 na ř. 17 shora je na levé straně rovnosti separabilní stav vyjádřený direktním součinem dvou operátorů hustoty a na pravé straně čistý entanglovaný stav vyjádřený pomocí ket-vektorů. To je hned několik chyb najednou.

- Hodnota na pravé straně první rovnice na str. 13 není správně. Pravděpodobně by tam mělo být $\frac{\sqrt{2}+1}{\sqrt{2}+2}$.

- Rov. 2.47 na str. 21. Pravá strana by měla pravděpodobně ještě obsahovat $p(y)$, tedy $H(X|Y) = -\sum_{x,y} p(y)p(x|y)\log(p(x|y))$.

- Na str. 35 se píše: „While DV-QKD was proven to work and is already commercially available, it has several disadvantages, for instance, high losses and limited reach ...". Především, ztráty jsou vlastností linky. V CV-QKD protokolech mají ztráty obvykle horší vliv než v DV (mění stav, čímž zvyšují chybovost). CV protokoly také obvykle dosahují kratších vzdáleností než DV protokoly. Na krátkých vzdálenostech ale mají větší přenosové rychlosti.

- Na str. 37 se píše, že no-clonning teorém limituje možnosti kvantových pamětí (protože kvantovou informaci nelze duplikovat). To ale není tak docela pravda. Existují kvantové opravné kódy, kdy je obecný stav qubitu zakódován do více qubitů.

- Dvě poznámky k podkapitole 3.2 na str. 41: PM vlákna nezachovávají obecný polarizační stav. Nemyslím, že systémy využívající fázové kódování jsou výrazně složitější nebo dražší. Největší komplikací je u nich nutnost průběžně stabilizovat fázové poměry.

- Podkapitola 3.2.2 na str. 46. Bylo by dobré uvést, že pro velké ztráty na lince není protokol B92 bezpečný. Eva může provádět *unambiguous state discrimination* a ztrátovou linku nahradit linkou ideální.

- Podkapitola 3.2.4 na str. 52. Zde se uvádí, že ke generování klíče dochází při kombinaci bází A_1, B_1. S ohledem na uvedenou definici bází se ale spíše jedná o A_2, B_1.

- Podkapitola 3.2.5 na str. 53. Z hlediska bezpečnosti nejsou protokoly BBM92 a E91 zcela ekvivalentní. Protokol E91 umožňuje tzv. *device independent QKD.*

- Při popisu útoků by bylo dobré rozlišovat, které útoky jsou „kvantové", cílené na ideální protokoly (ty vždy způsobí chyby) a které jsou „nekvantové", tedy využívající nedokonalostí implementace (ty chyby způsobit nemusejí, ale existují proti nim technická opatření).

- Na str. 62 se píše: „This is achieved by shortening the key length while increasing its entropy." Bylo by dobré upřesnit o entropii čeho se mluví. Entropie samotného klíče by i bez *privacy amplification* měla být maximální. Jde o snížení informace o klíči, kterou má Eva.

- Str. 66. Co se myslí pseudonáhodnými generátory založenými na náhodných procesech? Domnívám se, že jako pseudonáhodné se označují pouze algoritmické generátory.

- Odstavec pod rovnicí (4.16) na str. 71 je poněkud zavádějící. Eva se obvykle snaží získat co nejvíce informace, takže by chtěla, aby se poslední skalární součin blížil nule. Poslední věta odstavce je zjevně nepravdivá.

- Poznámka k PNS útoku: Eva také může zaměnit ztrátovou linku za bezztrátovou a blokovat část jednofotonových pulzů, čímž sníží QBER.

- V části věnované útokům nejsou vůbec zmíněny kolektivní a koherentní útoky.

- Str. 75 a 76. Metoda *decoy states* je zde popsána poněkud vágně. Přitom ji autor používá ve své simulaci. Podstatné u této metody je, že lze určit pravděpodobnost detekce v případě, že Alice poslala n-fotonový stav. Tyto pravděpodobnosti musejí být stejné pro signálové i *decoy* stavy. Zmíněné pravděpodobnosti se sice nedají přímo „měřit", ale lze je odhadnout ze znalosti četností detekce pro jednotlivé typy stavů.

- Na str. 85 se píše „For noise-less channel with an eavesdropper ..." Je třeba uvést, jaký konkrétní útok se zde simuluje.

- Na str. 86 se uvádí „This showcases the danger of PNS attack, because it may be unnoticed by Alice and Bob." V případě BB84 se slabými koherentními pulsy bez použití metody *decoy states* se musí počítat s tím, že všechny vícefotonové pulzy poskytují Evě veškerou informaci, kterou nesou. Tato potenciálně uniklá informace se musí vzít v úvahu při proceduře *privacy amplification.*

- V práci se vůbec nezmiňuje nutnost autentizace zpráv posílaných po klasickém otevřeném kanálu mezi Alicí a Bobem. Přitom je jasné, že bez autentizace by bezpečná distribuce kvantového klíče nebyla možná, protože útočník by mohl realizovat *man-in-the-middle attack*.

- Je škoda, že simulace nepočítá pro srovnání také obecné dolní a horní meze pro rychlost generace bezpečného klíče (viz např. [26]).

- Práce se nezabývá – ani teoreticky – otázkou aktivní stabilizace fáze v inretferometru. Bez fázové stabilizace nelze zařízení reálně provozovat.

Otázky:

- Na str. 7 je uveden příklad čistého separabilního stavu. Jak je definována separabilita pro obecné smíšené stavy?

- Rov. 2.19 na str. 10. Co značí M (bez indexu)?

- Je možné realizovat POVM pomocí projektivních měření?

- Rov. 2.30b na str. 12. Proč je zde 1/2? Je snad stav $|-\rangle$ nenormovaný? Nebo se liší apriorní pravděpodobnosti stavů $|\psi_0\rangle$ a $|\psi_1\rangle$?

- Str. 26, ř. 11 shora. Proč zde předpokládáte separabilní stav?

- Na str. 32 se píše „$\mathcal{B}^\varepsilon(\rho)$ represents the set of all quantum states ρ' that are within an ε-proximity to ρ." Jaká se zde uvažuje definice vzdálenosti?

- Str. 57. Jak se určí hodnota $P(\Lambda_k \leq \lambda_{\max})$?

- Na str. 72 se uvádí, že stav světla emitovaného laserem lze popsat smíšeným stavem ρ_μ. Za jakých podmínek to platí?

- Na str. 87 se uvádí „... there is still non-zero final key length ... However, this level of error correction potentially compromises the secrecy of the key by leaking significant amount of information." Co se tím míní? Po aplikaci algoritmu *privacy amplification* by klíč měl být vždy bezpečný (ε-bezpečný) anebo žádný.

- Z obr. 5.6 na str. 90 vyplývá, že když se započte šum, tak vychází delší bezpečný klíč. Můžete to vysvětlit?

- Str. 97, měření dělicích poměrů děličů svazku. Při jaké teplotě a na jaké vlnové délce měření probíhala? Zkoumal jste případnou závislost dělicího poměru na polarizaci?

- Str. 100. Nejvyšší hodnoty interferenčního kontrastu při měření autokorelační funkce se pohybovaly kolem 25%. Chápu, že nešlo o optimalizaci kontrastu, ale i tak je to hodnota velmi nízká. Co bylo příčinou tak nízké vizibility?

- Str. 101. Jak byl měřen interferenční kontrast v případě dvou nevyvážených interferometrů? Byly vybírány pouze pulzy odpovídající šíření krátkým-dlouhým a dlouhým-krátkým ramenem? (Pokud ne, mělo to být v textu uvedeno.)

- Str. 103. Za jakých okolních světelných podmínek byly měřeny četnosti temných impulsů detektorů?

- Str. 104. Byly výstupy detektorů a vstupy do mikrokontroleru impedančně přizpůsobeny, aby nedocházelo k přechodovým jevům?

Práce vyhovuje požadavkům kladeným na diplomovou práci a doporučuji ji k obhajobě.

I přes výše uvedené výhrady se domnívám, že se jedná o poměrně kvalitní práci, a navrhuji ji hodnotit známkou **C**.

V Olomouci dne 25. května 2024.

Prof. RNDr. Miloslav Dušek, Dr.
Katedra optiky, Přírodovědecká fakulta
Univerzita Palackého v Olomouci

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Quantum cryptography with time and phase encoding**
Jméno autora:	**Ondřej Čermák**
Typ práce:	diplomová práce
Fakulta:	Fakulta jaderná a fyzikálně inženýrská (FJFI)
Katedra:	Katedra laserové fyzika a fotoniky
Oponent práce:	Prof. RNDr. Miloslav Dušek, Dr.
Pracoviště oponenta práce:	Katedra optiky, Přírodovědecká fakulta, Univerzita Palackého v Olomouci

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Téma práce bylo relativně náročné. Bylo nutné nastudovat teoretické postupy z oblasti kvantové mechaniky a teorie informace a zvládnout experimentální metody kvantové optiky.

Splnění zadání **splněno**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Všechny body zadání lze považovat za splněné. Pokud jde o experimentální část, student se měl pokusit sestavit experimentální uspořádání, což splnil. Kompletní experimentální demonstrace kvantového přenosu klíče nebyla požadována.

Zvolený postup řešení **vhodný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Student zvolil správný postup řešení.

Odborná úroveň **průměrná**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Viz textovou část posudku.

Formální a jazyková úroveň **průměrná**

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Viz textovou část posudku.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Výběr zdrojů, korektnost citací	**průměrné**
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.	
Student použil poměrně velké množství pramenů. V textu by se však měl více soustředit na ty informace, které s tématem práce přímo souvisejí. Také by bylo vhodné více upřednostňovat citace původních zdrojů, které s určitou myšlenkou přišly, před citacemi pozdějších a přehledových prací.	

Další komentáře a hodnocení
Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.
Viz textovou část posudku.

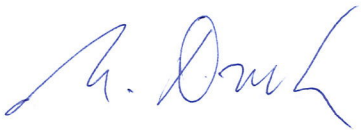
III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

K práci mám několik formálních i obsahových připomínek (viz textovou část posudku). Teoretická část práce obsahuje drobné chyby, experimentální část nebyla - pravděpodobně z časových důvodů - dotažena až k demonstraci kvantového přenosu klíče (jádro zařízení ale bylo postaveno). Na druhou stranu je nutno uvážit, že téma práce bylo relativně náročné. Z práce je také patrné, že student prokázal dostatečné porozumění teoretickým základům studované problematiky i potřebnou experimentální zručnost.

Práce vyhovuje požadavkům kladeným na diplomovou práci a doporučuji ji k obhajobě.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **C - dobře.**



Datum: 26.5.2024

Podpis: