FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Ivo Petr, Ph.D.
Student:	Michael Wagner
Název práce:	Protokoly pro kvantový přenos klíče
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	1. června 2023

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
- [2] zadání splněno s menšími výhradami
- [3] zadání splněno s většími výhradami
- [4] zadání nesplněno

Student nastudoval koncepty používané v kvantovém přenosu klíče a popsal princip protokolů BB84, B92 a E91. Ačkoliv se jedná o známé protokoly, v literatuře se běžně objevují pouze základní verze protokolů a student proto musel nastudovat větší množství původních článků. Hlavním přínosem práce je rešerše fungování protokolů a detekce odposlechu při provozu na nedokonalém kanále kde je nutné využití opravných kódů. K simulaci protokolů student využil SDK Qiskit, což mu umožnilo generovat ukázky průběhu ustanovení klíče v ideálním případě, s odposlechem a v přítomnosti chyb. Jakkoliv by práci šlo dále rozšiřovat o další aspekty vycházející z klasické a kvantové teorie informace, zadání považuji již ve stávající podobě za náročnější a přitom zcela splněné.

2. Písemná část práce

75 / 100 (C)

Text práce je logicky dobře členěný. Student se snaží čtenáři kromě samotných protokolů objasnit principy kvantové informatiky, teorie opravných kódů a principy posílení soukromí. To je ovšem v rámci bakalářské práce obtížné a text se např. u posílení soukromí nebo měření nutně dopouští zkratek, kdy se nedaří problematiku dostatčně objasnit. Použité příklady jsou užitečné a výklad dobře doplňují. Členění do definic, tvrzení a jejich důsledků by se nicméně dalo zlepšit, stejně jako práce s interpunkcí ve větách. Práce řádně cituje relevantní literaturu. Závěrečná kapitola popisující experimenty by si zasloužila rozšířit o podrobnější popis experimentů případně ukázky kódu.

3. Nepísemná část, přílohy 100 /100 (A)

Přílohou práce jsou Jupyter notebooky simulující ustanovení klíče pomocí SDK Qiskit. Kód je dobře srozumitelný, přehledný a se základní znalostí jazyka Python umožňuje prozkoumat princip popisovaných protokolů.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Práce popisuje známé protokoly pro kvantový přenos klíče, běžný popis základních verzí těchto protokolů ale obohacuje o důležité prvky komunikace v nedokonalém kanále s přítomností odposlechu. Vytvořené simulace text dobře doplňují a mohou sloužit jako výukové pomůcky a studijní materiály pro další studenty. Hodnocení drobně sráží některé nedostatky v textu.

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student aktivně vyhledával problémy objevující se v problematice kvantového přenosu klíče a pracoval na jejich řešení. Svůj postup pravidelně konzultoval a zapracovával zpětnou vazbu od vedoucího práce.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Student je schopen samostatné tvůrčí práce.

Celkové hodnocení 90 /100 (A)

Práce popisuje a v praktické části simuluje vybrané protokoly pro kvantový přenos klíče. Oceňuji že student nezůstal u základních verzí protokolů, ale přidal také aspekty, které se běžně v základní literatuře nezmiňují. Text práce by v některých pasážích zasloužil doplnit či zpřehlednit, vzhledem k náročnosti problematiky se ale nepřesnosti dají prominout. Celkkově práci považuji za zdařilou a doporučuji ji k obhajobě.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.