FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Mgr. Martin Jureček, Ph.D.
Student:	Michael Wagner
Název práce:	Protokoly pro kvantový přenos klíče
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	9. 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

Všechny body ze zadání považuji za splněné.

2. Písemná část práce 80 /100 (B)

Práce je dobře členěná a má odpovídající rozsah. Bibliografie obsahuje práce relevantní k tématu. Teoretické pojmy jsou uváděny ve formě definic a tvrzení. Některé teoretické pojmy mohly být lépe vysvětleny.
Seznam nedostatků:
- chybí specifikované zdroje, z nichž student převzal některé pasáže z teoretické části, např. část kapitoly 3.2 je převzata z článku [19], ale není to v textu uvedeno.
- v tvrzení 3.22 je uvedeno pravděpodobnostní rozdělení P_X, ale ve vzorci (3.24) vystupuje P_X jako pravděpodobnost náhodné veličiny X.
- obrázky 2.3a a 2.3b nejsou odkázány v textu a obrázek 1.1 je zmíněn v textu až o tři strany dále. Také tabulka 6.2 by mohla být uvedena v textu.
- str. 14: "Nicméně, protože jde stále o problémy matematického typu, nemůžeme si být jisti, že se nenajdou algoritmy, které dokáží tyto schémata efektivně rozbít [7]." - to je silné tvrzení.
- překlepy: např. ve vztahu (1.8) při definici pravděpodobnosti; dále "sdružená entropie" místo sdružená entropie (Def 3.24), nebo "úvést" (v Závěru).

3. Nepísemná část, přílohy 95 /100 (A)

Implementace je provedena v jazyce Python. Student pro simulaci protokolů využívá framework Qiskit. Zdrojové kódy mohly obsahovat více komentářů.

4. Hodnocení výsledků, jejich využitelnost 85 /100 (B)

Práce přehledně prezentuje protokoly pro kvantový přenos klíče. Přínosem práce je také poměrně velké množství řešených příkladů, které demonstrují teoretickou část. Experimentální část z pochopitelných důvodů nebyla provedena na kvantovém počítači, ale jen na jeho simulátoru. Práce studenta může sloužit jako základ pro budoucí rozšiřující práce.

Celkové hodnocení 91 /100 (A)

Text práce obsahuje drobné nedostatky, avšak ty nesnižují její čitelnost. Protokoly pro kvantový přenos klíče jsou poměrně detailně zpracovány a text práce je doplněn o množství řešených příkladů, což je přínosem práce. Experimentální část byla poměrně jednoduchá, avšak dobře zpracovaná. Celkově práci studenta hodnotím známkou A.

Otázky k obhajobě

1. Teoretické části textu, u kterých není uvedeno, že byly převzaty z nějakého zdroje, připravoval student sám, nebo je převzal z nějakého zdroje a zapomněl to uvést v textu?
2. Práce obsahuje experimenty se třemi algoritmy pro kvantový přenos klíče. O jaké další algoritmy by student navrhoval rozšířit jeho práci?

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.

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.