FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Mgr. Martin Jureček, Ph.D.
Student:	Kryštof Nevšímal
Název práce:	Možnosti aplikace důkazu s nulovými znalostmi v praxi
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	10. června 2024

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 práce považuji za splněné.

2. Písemná část práce 91 /100 (A)

Práce je dobře členěná a má odpovídající rozsah. Text obsahuje menší počet nedostatků, které však nebrání v čitelnosti.
Zde je uveden nekompletní seznam:
- reference je samostatné slovo a nepíše se spolu s jinými slovy
- z definice vlastnosti úplnosti v kap. 1.2 vyplývá, že pokud dokazující zná tajemství, tak se 100% pravděpodobností přesvědčí ověřovatele. Avšak v příkladu "Barvoslepý kamarád" z kap. 1.3.1 se uvádí "Na druhou stranu, pokud Alice stokrát odpoví správně, nakonec se jí podaří přesvědčit Boba na základě pravděpodobnosti, že mezi míčky je rozdíl.", což je ve sporu se studentovou definicí úplnosti.
- také se mi zdá, že příklad "Barvoslepý kamarád" je nesprávně definovaný a neshoduje se s příkladem z [3], o kterém student tvrdí, že ho převzal. Konkrétně jde o větu "Bud' byly míčky různobarevné a pravděpodobnost, že Alice odpoví správně, je 100 %, nebo měly stejnou barvu a pravděpodobnost, že Alice zvolí náhodně ten správný, je 50 %." Pokud Alice dokáže rozlišovat barvy, jak je zřejmé z kontextu, tak nemá důvod volit náhodně, jak student tvrdí v textu. Tento důvod má barvoslepý útočník, který se vydává za Alici.
- některé obrázky nejsou zmíněny v textu (např. obr. 1.1 nebo obr. 1.3)
- ve větě "Co se týče postkvantové odolnosti, Eli Ben-Sasson uvádí,,..." se má uvést reference a ne jen jméno autora
- v kap. 2.2.2.1 v definici grupy G chybí složené závorky
- Definice 1.1. je doslova převzatá z [19]

- v textu se vyskytuje neformální vyjadřování, které do odborného textu nepatří
Celkově je ale práce čtivá a čtenáři poskytuje základy pro pochopení důkazů s nulovou znalostí a jejich použití.

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

Implementace je napsána v jazyku Rust, což je pro danou problematiku vhodná volba a celkově k nepísemné části nemám žádné výhrady.

4. Hodnocení výsledků, jejich využitelnost 92 /100 (A)

Práce může být použita jako dobrý zdroj obsahující úvod do důkazů s nulovou znalostí a demonstraci jejich použití v různých aplikacích.

Celkové hodnocení 93 /100 (A)

Student teoretickou i praktickou část práce zvládl výborně. V písemné části se vyskytlo několik nedostatků, které ale příliš při čtení neruší a jsou spíše menšího významu. Z výše uvedených komentářů hodnotím práci známkou A - výborně.

Otázky k obhajobě

Jaká má být správná definice vlastnosti úplnosti, aby byla v souladu s příkladem "Barvoslepý kamarád"?
Jak by se dala tato bakalářská práce rozšířit, aby z ní mohla vzniknou navazující diplomová práce?

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.