FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Mgr. Martin Jureček, Ph.D.
Student:	Arnold Stanovský
Název práce:	Analýza Percy++, knihovny pro Private Information Retrieval
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	21. srpna 2023

Hodnotící kritéria

1. Splnění zadání

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

Všetky body zo zadania práce považujem za splnené.

2. Písemná část práce 70 / 100 (C)

Práca je dobre štrukturovaná a má odpovedajúci rozsah. Text práce obsahuje niekoľko nedostatkov:
- v definícii 1.1 nie je PIR problém definovaný presne. Bolo treba špecifikovať, že ide o i-tý bit reťazca x. Taktiež definícia PIR problému definuje "k" databáz, ale toto "k" sa ďalej v definícii nepoužíva.
- v texte je uvedených niekoľko algoritmov, pričom len niektoré z nich boli prezentované v tvare pseudokódu. Len u jedného algoritmu bol uvedený demonštrujúci príklad, avšak ten bol prevzatý z článku [4].
- pseudokód algoritmu na str. 10 nie je odkázaný v texte a v kroku 2 chýba podmienka, že alpha_i musia byť po dvoch rôzne
- tabuľka 1.1 a obrázok 1.4 zasahujú za okraj
- úroveň angličtiny je dobrá, chyby sa týkajú hlavne čiarok a členov
- práca je písaná v prvej osobe jednotného čísla (napr. "I will now describe") a používa sa aj prvá osoba množného čísla (napr. "We have observed")

3. Nepísemná část, přílohy 90 / 100 (A)

Jednotlivé protokoly boli importované z knižnice Percy++. Vzhľadom k zadaniu práce by som očakával viac informácii o knižnici, avšak nenašiel som v práci na ňu ani odkaz. Experimentálne výsledky je možné overiť.

4. Hodnocení výsledků, jejich využitelnost 80 /100 (B)

Práca prezentuje hlavné PIR protokoly a môže byť ďalej rozšírená o ďalšie protokoly, ktorých implementácie by mohli rozšíriť knižnicu Percy++. Prínosom práce je ďalej experimentálna časť, ktorá obsahuje analýzu bezpečnostných vlastností a výpočtových nárokov jednotlivých protokolov.

Celkové hodnocení 77 /100 (C)

Z textu práce nie je vždy jasné, čo je prevzaté a čo je prínosom študenta. Pretože len u jedného algoritmu bol uvedený demonštrujúci príklad, avšak ten bol prevzatý z článku [4], tak vzniká otázka či študent uvedeným algoritmom skutočne rozumie, alebo ich len odpísal z článkov a aplikoval ich implementácie z knižnice percy++ bez hlbšieho porozumenia. Experimentálna časť bola pomerne jednoduchá, avšak dobre spracovaná. Celkovo prácu študenta hodnotím známkou C.

Otázky k obhajobě

1. Na strane 6 je uvedené, že prvočíslo p musí byť väčšie ako 2^(3w_AG). Prečo je nutná táto podmienka?
2. Ako presne sa aplikuje kódovanie aj dekódovanie v prípade Goldbergovho algoritmu?
3. Plánuje študent rozšíriť knižnicu Percy++ o implementácie nových protokolov?

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.