FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Mgr. Martin Jureček
Student:	Bc. Jana Berušková
Název práce:	Redukování předefinovaných systémů polynomiálních rovnic odvozených ze zjednodušených variant AES
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	15. září 2022

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 95 / 100 (A)

Študentka kvalitne spracovala pomerne náročnú tému. Práca je dobre členená a v texte sa vyskytuje minimálny počet preklepov. Uvedené zdroje sú relevantné a práca má odpovedajúci rozsah.

3. Nepísemná část, přílohy 97 / 100 (A)

Študentka upravila existujúce skripty na generovanie rovníc, rozšírila ich a naimplementovala postupy redukcie predefinovaných sústav polynomiálnych rovníc nad GF(2). Pri výpočte Groebnerových báz využila software Magma. Experimenty popísané v práci je možné zopakovať a overiť ich správnosť.

4. Hodnocení výsledků, jejich využitelnost 93 / 100 (A)

Práca nadväzuje na minuloročnú diplomovku Ing. Bielika, ktorá bola základom pre článok publikovaný na konferencii. Pretože študentka niektoré výsledky ešte zlepšila, jej diplomová práca má taktiež potenciál k publikácii.

5. Aktivita studenta

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

Študentka pravidelne konzultovala s vedúcim práce najnovšie výsledky a ďalšie kroky počas celého obdobia práce bez väčších časových okien.

6. Samostatnost studenta

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

Študentka si sama naštudovala teóriu Groebnerových báz a podarilo sa jej za pomoci Marka Bielika rozšíriť jeho skripty na generovanie rovníc. S vedúcim konzultovala vhodné postupy na spracovanie rovníc, ktoré sama naimplementovala.

Celkové hodnocení

95 /100 (A)

Prácu hodnotím po teoretickej aj praktickej časti ako nadpriemernú. Študentka dosiahla výsledky, ktoré majú potenciál k publikovaniu. A preto prácu hodnotím známkou A.

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.