FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš
Student:	Bc. Hana Svobodová
Název práce:	Pokročilé algoritmy pro sdílení tajemství
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	16. května 2022

Hodnotící kritéria

1. Splnění zadání

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

Studentka navázala na svoji bakalářskou práci a zpracovala problematiku ve velmi vysoké kvalitě. K základním algoritmům zformulovala jejich hlavní nedostatky a možné útoky na ně, a provedla důkladnou rešerši algoritmů, které tyto nedostatky řeší. Tyto pak srozumitelně popsala a následně naimplementovala v podobě jednoduše použitelné knihovny.

2. Písemná část práce 100 / 100 (A)

Textová stránka práce je vynikající. Studentka provází čtenáře problematikou v logické posloupnosti a hutným, ale srozumitelným způsobem ho uvádí do kontextu. Práce je mimořádně solidně podložena, všechna tvrzení jsou doprovázena důkazy, příklady, analýzou možných problémů. I po jazykové stránce je text výborný.

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

Také nepísemná část práce je výborná. Studentka připravila implementaci všech nastudovaných algoritmů v podobě jednoduše použitelné knihovny, a také demonstrační aplikaci, na které si je uživatel může snadno vyzkoušet. K dispozici je i Pythonový program pro simulaci kvantového sdílecího algoritmu. Kvalita kódu je obecně velmi vysoká, kód je přehledný, dobře zdokumentovaný a velmi důkladný. Jedinou drobnou výhradu mám k tomu, že pro demonstraci algoritmu BGW by bylo lepší rozdělit obě jeho fáze do samostatně proveditelných kroků s výpisem mezivýsledků, aby si uživatel mohl vyzkoušet, že skutečně žádný z ostatních účastníků výpočtu neuvidí jeho tajnou hodnotu.

Ideálně také mohla být provedena demonstrace "elektronických voleb" s uživatelsky definovaným počtem účastníků.

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Výsledkem práce je mimořádně důkladná rešerše předmětné oblasti a vytvořené programové vybavení, které ji dovolí snadno používat i člověku, který se v jejím teoretickém pozadí neorientuje. Pravda je, že praktické využití se týká poměrně specifické oblasti, kterou nepotřebuje každý, pokud ale zrovna čtenář narazí na potřebu řešit problémy popisované v práci, najde v ní všechno, co k tomu potřebuje.

5. Aktivita studenta

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

6. Samostatnost studenta

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

Celkové hodnocení 95 /100 (A)

Práce je po všech stránkách výborná. Je velmi důkladně podložena teorií, kterou srozumitelně sděluje čtenáři a následně velmi kvalitně implementuje do podoby snadno použitelné knihovny i názorného demonstračního programu. Velkým přínosem je i zohlednění vlivu kvantových počítačů, jak ve vztahu k bezpečnosti popisovaných klasických algoritmů, tak ve vztahu k implementaci kvantového schématu pro rozdělení tajemství. Domnívám se, že jde o vhodného kandidáta pro zvážení na cenu děkana.

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.