FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Buček, Ph.D.
Student:	Bc. Ivana Trummová
Název práce:	Analýza složitosti binárních algoritmů pro modulární inverzi
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	2. června 2021

Hodnotící kritéria

1. Splnění zadání

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

Zadání je náročné, vyžaduje samostatně prostudovat a analyzovat odborné články a také navrhnout vlastní úpravu algoritmu pro výpočet modulární inverze.

2. Písemná část práce 80 / 100 (B)

Práce je stručná (s 45 stranami bez příloh je mírně pod spodní hranicí doporučeného rozsahu), ale obsahuje všechny nezbytné části. Práce je psána srozumitelnou angličtinou, studentka by se však měla vyhnout použití zkrácených forem (it's).

Po věcné stránce práci hodnotím pozitivně. Zejména vyzdvihuji studentkou vytvořený alternativní důkaz algoritmu 3 (Left shift inverse) a odhalení chyby v algoritmu Tao Wu.

Na druhou stranu mám výhrady k volbě způsobu testování jednotlivých algoritmů. Zvolená bitová délka operandů (1 až 14 bitů) neodpovídá reálnému použití (stovky až tisíce bitů). V praxi je také bitová délka prvočísla dána předem jako parametr, a je tedy otázka, zda se mají do sebe míchat výsledky běhu algoritmů s prvočísly různých délek.

Formální stránka práce má také svoje nedostatky. Studentka místy odkazuje na algoritmy pouze číslem, např. "in 1" místo "in Algorithm 1". Pojmenování "Montgomery Algorithm" je nejednoznačné, lepší by bylo "Montgomery Inverse Algorithm". Dále se místy studentka spoléhá na barevnou podobu práce, aniž by uvážila možnost, že bude někdy vytištěna nebo zobrazena jen černobíle nebo ve stupních šedi.

V seznamu literatury chybí přinejmenším odkaz na původní článek o Montgomery Inverse algoritmu (Kaliski, Burton S. "The Montgomery inverse and its applications." IEEE

transactions on computers 44.8 (1995): 1064-1065.).
Studentka uvádí Kaliskiho algoritmus jako by byl derivátem Montgomery Inverse algoritmu, ale byl to právě Kaliski, kdo algoritmus popsal a pojmenoval po Peteru Montgomerym.

3. Nepísemná část, přílohy 85 /100 (B)

Přílohou jsou jednak výpisy algoritmů s vyznačenými operacemi pro analýzu složitosti, dále příklady pro korekci chyby nalezené autorkou v algoritmu Tao Wu, a dále zdrojové kódy testovacích programů v jazyce C. Zdrojové kódy by zasloužily důkladnější popis a případně i nějaký skript, kterým by se měly programy spouštět, abychom získali statistické údaje, které studentka použila v práci.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Výsledky práce studentky zahrnují jednak analýzu operační složitosti vybraných algoritmů pro výpočet modulární inverze, dále alternativní důkaz algoritmu 3 (Left shift inverse), a v neposlední řadě odhalení a opravu chyby v algoritmu Tao Wu. Pomocným výsledkem jsou také programy v jazyce C implementující jednotlivé algoritmy za účelem pořízení dat pro analýzu operační složitosti.
Zejména odhalení chyby v algoritmu Tao Wu je výsledek, který má i publikační potenciál.

Celkové hodnocení 89 /100 (B)

Studentka prokázala schopnost samostatného studia, analýzy i tvůrčí práce a vytvořila hodnotný výsledek.
Přes uvedené výhrady práci doporučuji k obhajobě a hodnotím velmi dobře.

Otázky k obhajobě

V analýze složitosti algoritmu Left shift inverse jste do seznamu operací nepočítala redukční operátor OR na řádcích 4 a 9 (str. 52). Do jaké kategorie byste ho zařadila ve své analýze?

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. 26/2017, 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.