FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Jakub Dvořák
Oponent práce:	Mgr. Martin Jureček
Název práce:	Faktorizace pomocí eliptických křivek
Obor:	Počítačová bezpečnost

Datum vytvoření: 23. 1. 2021

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
Všetky body popísané v pokynoch pre vypracovanie práce považujem za splnené.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*75 (C)*

Popis kritéria:
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.

Komentář:
Predložená práca je pomerne rozsiahla a po matematickej stránke patrí medzi náročnejšie. Uvedené zdroje sú relevantné, ich zoznam je pomerne široký, avšak ich formát nie je vždy jednotný. Práca obsahuje pár desiatok preklepov a ďalších chýb, napr.: homogenizovaná rovnica zo str. 8., neutrálny prvok a výraz P+Q v Def. 14., hodnoty v Tab 1.2, na str. 23: "pracovat s tělesem GF(p) nad eliptickou křivkou", na str. 29 je prvok Q(x_i) z okruhu Z_n považovaný za reláciu, atď. Ďalej v práci chýba definícia neutrálneho prvku O a Galoisovo teleso je definované len pre prvočíselné rády. V práci sa vyskytuje neformálne vyjadrovanie: napr. str. 13: "...násobení a mocnění, což by měly být náročnější operace".

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*95 (A)*

Popis kritéria:
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

Komentář:
Implementácia bola vykonaná v jazyku C++ a boli využité knižnice OpenMP a OpenMPI pre paralelizáciu výpočtov. Všetky použité technológie sú adekvátne. Všetky dosiahnuté experimentálne výsledky je možné overiť.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*85 (B)*

Popis kritéria:
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.

Komentář:

Výstupom práce je porovnanie Weierstrassovho a Edwardsovho modelu. Vzhľadom k obmedzeniu 10 minút na každú úlohu si študent musel zvoliť pre testovacie účely najviac 130 bitové čísla, čo je pomerne málo. Pre porovnanie, minulý rok študent ČVUT FIT obhájil BP, v ktorej sa venoval faktorizácii až 400 bitových čísel. Oceňujem navrhnutú a podrobne popísanú implementáciu a paralelizáciu výpočtov, ktorá by mohla byť podkladom pre ďalšie rozšírenie práce.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

1. Na str. 30 je uvedené: “Snažíme se nalézt řešení kongruence Q(x_1)a_1 + Q(x_2)a_2 + · · · + Q(x_n)a_n = 0 (mod 2)”. Prečo sa o to snažíme?

2. Příklad z kap. 3.3.3.1 obsahuje chyby. Ako má vyzerať správne riešenie príkladu v zmysle algoritmu 4?

3. Prečo je Tvrdenie 3.3.1 dôležité pre GNFS a ako presne je využité v tomto algoritme?

4. Sú algoritmy 5,6,7 dielom študenta alebo sa študent inšpiroval z nejakého zdroja, ktorý nie je uvedený?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Celkové hodnocení

80 (B)

Popis kritéria:
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.

Text hodnocení:

Daná problematika spolu s experimentami bola spracovaná pomerne obšírne. Študentovi očividne viac vyhovuje práca implementačného ako teoretického charakteru. Vzhľadom k vyššie uvedeným chybám v texte prácu hodnotím známkou na hranici medzi B a C.

Podpis oponenta práce: