FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Matyáš Hollmann
Oponent práce:	Mgr. Martin Jureček
Název práce:	Summation polynomials and the discrete logarithm problem on elliptic curve
Obor:	Počítačová bezpečnost

Datum vytvoření: 29. 5. 2019

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:
Práca sa venuje problému diskrétneho logaritmu (PDL) na eliptických krivkách. Okrem známych algoritmov sú v práci spracované aj nové algoritmy založené na tzv. sumačných polynómoch. Práca obsahuje i realizáciu a experimentálne výsledky. Všetky body popísané v pokynoch pre vypracovanie považujem za splnené.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*98 (A)*

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:
Napriek pomerne náročnej téme sa študentovi podarilo prehľadne spracovať danú problematiku. Zvlášť kladne hodnotím štýl vysvetľovania jednotlivých algoritmov, kde je priamo do pseudokódov zahrnuté i podrobnejšie vysvetlenie. Práca obsahuje pomerne málo nedostatkov:
* študent si príklady (na str. 14 a 18) mohol vymyslieť aj sám a neodpisovať ich z knihy a navyše s chybou
* v Definícii 2.1.2 sa predčasne používajú pojmy ako jednotkový prvok alebo aditívny inverzný prvok. Tieto pojmy by sa mali používať až po Tvrdení 2.1.1, kde je uvedené, že množina bodov na eliptickej krivke tvorí grupu.
* ďalej je v práci niekoľko preklepov, ktorých počet je ale relatívne malý

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*98 (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:
Pri výpočte Algoritmov 1 a 2 (kap. 3) bolo potrebné spočítať Groebnerové bázy. Študent vyskúšal niekoľko existujúcich implementácií prostredníctvom systému SageMath a podarilo sa mu dopočítať výsledky v relatívne krátkom čase. Všetky uvedené experimenty je možné zopakovať a overiť namerané výsledky.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*98 (A)*

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:

Jedným z výsledkov práce je prehľadný popis moderných metód založených na sumačných polynómoch. Ďalším výsledkom je implementácia uvedených algoritmov, kde študent musel otestovať niekoľko existujúcich implementácií pre výpočet Groebnerových báz.

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:

* Mohol by študent presnejšie špecifikovať, ktoré všetky open-source implementácie Groebnerových báz testoval a aké s nimi mal skúsenosti? Skúšal študent použiť i komerčné programy ako napr. Mathematica alebo Maple pri výpočte groebnerových báz?
* Aké študent vidí potencionálne oblasti výskumu, ktoré by mohli byť pokračovaním tejto diplomovej práce?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*98 (A)*

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:

Študentovi sa podarilo prehľadne spracovať zložitejšiu problematiku a taktiež experimentálne otestovať jednotlivé algoritmy. Preto predloženú diplomovú prácu hodnotím známkou A.

Podpis oponenta práce: