FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Matyáš Hollmann
Vedoucí: práce:	Ing. Ivo Petr, Ph.D.
Název práce:	Summation polynomials and the discrete logarithm problem on elliptic curve
Obor:	Počítačová bezpečnost

Datum vytvoření: 28. 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:
Zadání bylo náročnější, přesto bylo zcela splněno. Student nastudoval a popsal současné metody řešení diskréního logaritmu v grupě bodů eliptické křivky. Dále implementoval několik variant algoritmů typu index calculus využívajících sumační polynomy a porovnal jejich výkon se standardně využívanými metodami.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*100 (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:
Písemná část práce je logicky dobře strukturovaná. Jelikož se jedná o oblast aktivního výzkumu, je třeba ocenit, že student uceleně objasňuje jak základy tak současný stav věci. Práce tedy může čtenáři sloužit jako úvodní studijní text. Po věcné i formální stránce práce vyhovuje nárokům na diplomovou práci. U převzatých výsledků student řádně cituje zdroje. Při analýze složitosti algoritmů na několika místech navíc doplňuje informace které v odborných textech chybí.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*100 (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:
Student implementoval několik verzí algoritmu řešícího ECDLP pro eliptickou křivku nad tělesem prvočíselného řádu. Pro implementaci byl zvolen open-source matematický software SageMath založený na Pythonu, který je vybaven širokou škálou vhodných knihoven potřebných zejména při práci s Groebnerovými bázemi. Student otestoval implementace v různých knihovnách a na základě testů zvolil nejlepší řešení. Výsledky testů vykonnosti jsou srovnatelné nebo lepší než výsledky uváděné v současných odborných článcích.

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

Práce podává ucelený přehled problematiky a může sloužit jako základ k dalšímu studiu metod index calculus pro řešení DCDLP. Potvrzuje, že v současném stavu není řešení založené na sumačních polynomech lepší než běžně používané metody (např. Pollard rho). Zlepšování dílčích kroků je však možné a jako výchozí bod může sloužit implementace vytvořená v této práci.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student nastudoval odbornou literaturu pouze s minimální pomocí školitele. Svůj postup pravidelně konzultoval, sám navrhnul a realizoval implementaci algoritmů.

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

Text práce je velmi kvalitní a srozumitelný přestože se jedná o složitou problematiku. Při popisu algoritmů student vysvětluje důležité myšlenky a diskutuje volby parametrů které literatura běžně opomíjí. Implementace je rovněž srozumitelná a efektivní, což potvrzuje porovnání s výsledky uváděnými v literatuře.

Podpis vedoucího práce: