FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Martin Holec
Vedoucí: práce:	Ing. Ivo Petr, Ph.D.
Název práce:	Babystep-Giantstep Algorithm and Solution of Elliptic Curve Discrete Logarithm Problem
Obor:	Počítačová bezpečnost

Datum vytvoření: 28. 1. 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:

Student se zabýval problematikou eliptických křivek a způsoby řešení problému diskrétního logaritmu v grupě bodů eliptické křivky (ECDLP) pomocí různých variant algoritmu Baby-step Giant-step (BsGs). V jazyce Julia implementoval algoritmy pro generování eliptických křivek, hledání řádu eliptické křivky a především různé varianty algoritmu BsGs, jejichž efektivitu porovnával při náhodně generovaných instancích ECDLP. Zároveň porovnával efektivitu řešení ECDLP při použití různých modelů eliptických křivek (Weierstrassův, Montgomeryho, Edwardsův). Výsledky měření jsou dobře zpracovány a po stránce implementace bylo zadání splněno. Kvalitu práce bohužel kazí písemná část práce, která je značně nepřehledná a nezasvěcený čtenář má velký problém se v práci vyznat. Z toho důvodu je pro čtenáře také těžké ocenit rozsah práce kterou student odvedl a která je nezanedbatelná.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*50 (E)*

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:

Práce postupně představuje čtenáři problém diskrétního logaritmu, eliptické křivky a varianty BsGs algoritmu. Praktická část práce popsaná v kapitole "Implementation" obsahuje celou řadu netriviálních teoretických výsledků, které by bylo vhodné vyčlenit do samostatné kapitoly. Jinak je práce logicky dobře strukturovaná. Po formální stránce bohužel obsahuje řadu nedostatků. Některé pojmy jsou použity dříve než jsou vysvětleny nebo se v průběhu práce několikrát změní jejich značení. Tento problém je markantní např. v kapitole 2, kde je při definici DPL použito symbolů y a beta pro stejnou veličinu aniž by na to byl čtenář upozorněn. V kapitole 4 je pro stejné veličiny použito symbolů P a Q, opět bez předchozího varování. Navíc dochází místy k míchání multiplikativní a aditivní notace pro grupovou operaci. Nejzávažnější zanedbání jsou zřejmě v kapitole 4, kde jsou algoritmy popsány povrchně a v pseudokódu dokonce špatně, jelikož místo veličin n0, n1, příp. n2 je všude použito n0. Zdroje student cituje v souladu s citačními zvyklostmi, pouze reference [1] a [15] (na straně 9) jsou poněkud úsměvné. Po jazykové stránce je text srozumitelný ale prospěla by mu jazyková korektura.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*80 (B)*

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:

Implementace jednotlivých porovnávaných variant BsGs sama o sobě není složitá, student se ale musel vypořádat nejen s nimi, ale také s generováním eliptických křivek v různých formách a zejména výpočtem jejich řádu, což celkovou náročnost zvyšuje. Praktická část práce je odvedena kvalitně.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*80 (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:

Práce zkoumá kromě různých variant BsGs algoritmu také výkonnost algoritmů při použití různých forem eliptických křivek. Zajímavým výsledkem je vliv kofaktoru řádu křivky na výkon algoritmů. Pokud je mi známo, není tento vliv v literatuře popsán. Pokud by se tento efekt povedlo potvrdit a vysvětlit, má práce publikační potenciál a případně může mít praktické důsledky.

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:

Oceňuji, že student navrhl zkoumání vlivu kofaktoru řádu eliptické křivky na výkonnost algoritmů. Efekt se bohužel nepovedlo vysvětlit. V praktické části student postupoval velmi samostatně. Text práce ovšem vznikal pod velkým časovým tlakem a na práci je to znát, viz hodnocení písemné části práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*65 (D)*

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:

Student splnil zadání v praktické části práce a přinesl zajímavé výsledky. Celkové hodnocení zhoršují výhrady k písemné části diplomové práce.

Podpis vedoucího práce: