FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Peter Bočan
Oponent práce:	prof. Ing. Pavel Tvrdík, CSc.
Název práce:	Symplectic Orthogonalization and Lattice Reduction Techniques
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 12. 6. 2018

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:
Úkolem BP bylo provést teoretickou analýzu matematických základů kryptografických metod veřejného klíče založené na faktu, že v n-rozměrných celočíselných mřížích (lattices) je problém nalezení nejmenšího vektoru faktoriálně složitý. Student věnoval této analýze hodně úsilí, zpracoval ji do 4 kapitol, Teorie mříží, Ortogonalizace báze mříží, popis vlastní kryptografie veřejného klíče NTRU a konečné Symplektické a duálně ortogonalizační algoritmy. Celkově svojí teoretickou náročností tato analýza přesahuje náročnost BP, student potřeboval komprimovat poměrně složité matematické struktury a algoritmy sepsat do uceleného výkladu za cenu mnoha zjednodušení ale při zavedení vlastní sjednocující terminologie a notace. Tyto 4 kapitoly splnily prvni 2 body zadaní, byť mají své nedostatky. Nicméně třetí bod je splněn nedostatečně, implementace a prověření složitosti ortogonalizačních algoritmů jsou minimalisticky popsány formou 2 dvoustránkových kapitol Implementace a Výsledky. Evidentně z časových důvodů. Student základní sadu ortogonalizačních algoritmů implemenoval, je na přiloženém memory-sticku, nicméně písemná část práce neobsahuje ani popis implementované knihovny ani výsledky testů vyjma několika nejjednodušších.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*65 (D)*

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:
Čtyři rešeršní kapitoly představující teoretické jádro práce obsahují různé nejasnosti, překlepy a myšlenkové skoky. Text je na některých místech příliš stručný, v podstatě série definic a vět bez důkazů. Původní záměr vytvořit přehledovou studii vysvětlující NTRU kryptologii se tím zdařil pouze částečně, protože je pro čtenáře, který tuto problematiku nemá nastudovanou, v řadě pasáží nesrozumitelný. Např. poslední odstavec Kap. 3 formuluje závěry bez vysvětlení. Nejméně sruzumitelná je Kap.4 o symplektických mřížích, uvedené algoritmy nejsou okomentovány ani formálně analyzovány, takže není zřejmé, zda korektně implementují ortogonalizaci symplektických mříží. Na druhou stranu je třeba vzít v úvahu, že se jedná o matematiku výrazně přesahující náročností témata probíraná na bakalářském stupni. Kapitoly 5 Implementace a Kapitole 6 Výsledky jsou dvoustránkové, zjevně psané na poslední chvíli. Přestože elnická příloha obsahuje implemenaci všech popsaných algoritmů, text práce prezentuje pouze elementární testy na prostorech malé dimenze do 100, kde jsou běhové časy řádu jednotek vteřin. Naimplemenovaná knihovna není popsaná a obecbě tedy chybí popis výkonnostních testů ortogonalizačních algoritmů na NTRU mřížích, který byl 3.požadavkem zadání..

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*65 (D)*

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:

Dokumentace v práci nebyla popsaná, příloha obsahuje kódy, hodnotím jako předchozí bod.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*65 (D)*

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:

Teoretická část by potřebovala rozšířit o příklady, myšlenky důkazů tvrzení a vysvětlení souvislostí pseudokódů algoritmů a teoretických podkladů, pak by se práce mohla stát pomůckou pro zájemce o porozumění NTRU kryptografii.

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:

Popište architekturu implementované knihovny algoritmů a závěry z výkonnostních testů.

Přeformulujte srozumitelněji závěry, stávající kapitola Conclusion obsahuje věty, které nedávají smysl.

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:

Téma je teoreticky (matematicky) náročné, přesahující rámec témat bakalářského základu, student se s různými výhradami zhostil dobře, bohužel z časových důvodů nebyly dokončeny výkonnostní testy a zdokumentovaná implementovaná knihovna . Chybí tedy i celkové zobecnitelné hodnocení výsledků.

Podpis oponenta práce: