FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Peter Bočan
Vedoucí práce: Ing. Ivo Petr, Ph.D.
Název práce: Symplectic Orthogonalization and Lattice Reduction Techniques
Obor: Bezpečnost a informační technologie

Datum vytvoření: 10. 6. 2018

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* ***2=náročnější zadání,*** *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Úkolem studenta bylo prostudovat základy teorie mřížek a jejich aplikace v kryptografii. Zejména se student měl zaměřit na asymetrický šifrovací systém NTRU a speciální typ mřížek který se objevuje v analýze bezpečnosti NTRU. Jelikož se nejefektivnější známé metody pro nalezení soukromého klíče spoléhají na redukci (ortogonalizaci) báze mřížky, měl student prozkoumat, implementovat a porovnat efektivitu ortogonalizačních algoritmů. Zadání shledávám náročnějším, protože student musel nastudovat rozsáhlou teorii mřížek a postupy ortogonalizace, přičemž musel čerpat nejen z učebnic, ale i z odborných článků. Navíc, přestože samotné algoritmy nejsou složité, bylo potřeba implementovat několik jejich variant a porovnat jejich výkon.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Student nastudoval základy teorie mřížek, stávající ortogonalizační algoritmy i princip systému NTRU. Text práce je ale silně nedostačující. Student implementoval studované algoritmy v jazyce C++ a provedl porovnání časů běhu některých z nich. K tomu musel také vytvořit náhodný generátor instancí řešeného problému (tzn. NTRU mřížek). Z popisu testování není jasné jak testování probíhalo, s jakými parametry a proč. Algoritmy byly testovány na mřížkách dimenze nejvýše 100, kde se ale rozdíly jednotlivých variant téměř neprojevily.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	*1=splňuje požadavky,* *2=splňuje požadavky s menšími výhradami,* ***3=splňuje požadavky s většími výhradami,*** *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Písemná práce zaměřená na toto téma by si zasloužila větší rozsah a to především u kapitol týkajících se testování algoritmů a interpretace výsledků. Algoritmy uvedené v kapitole 2 a 4 jsou mnohdy popsány jen pseudokódem, chybí komentáře a vysvětlení uváděných postupů. Mnohdy chybí i účel daného algoritmu a jeho souvislost s problémem ortogonalizace. Kapitola 4, která má osvětlit nejsložitější koncepty je psána téměř heslovitě.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*40 (F)*

Popis kritéria:
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.

Komentář:

Téma klade velké nároky na správnost formulací i logickou strukturu práce a pro studenta bakalářského programu je obtížné dosáhnout potřebné úrovně. Předložený text práce je ovšem plný věcných chyb což orientaci čtenáře velmi ztěžuje. Mnohá vysvětlení chybí, objevují se nedefinované pojmy jako např. "dobrá" a "špatná" báze, "span Lambda". Pojmy jako objem mřížky jsou sice definovány, ale dále nepoužity. Značení použité v práci není konzistentní.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*40 (F)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Komentář:

Po formální stránce je práce velmi nedotažená. Kromě nejednotné notace obsahuje celou řadu gramatických chyb, mnohdy chybí celá slova či části vět. Práce by zasloužila jazykovou korekturu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*100 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:

Práce cituje především odbornou literaturu a aktuální výzkumné články a na patřičných místech se na ni odkazuje.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*70 (C)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:

Práce měla především rešeršní charakter a jejím cílem bylo v první řadě rekonstruovat výsledky obsažené v článku [5] citovaném v práci. Testování na mřížkách malé dimenze neprokázalo výhody symplektických verzí algoritmů proti jejich standardním verzím.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:

Dosažené výsledky částečně rekonstruují známé výsledky. Potenciál rozšířit studium o zkoumání závislosti výkonu algoritmů na dalších parametrech se nepovedlo naplnit.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* ***3=průměrná aktivita,*** *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: *1=výborná samostatnost,* *2=velmi dobrá samostatnost,* ***3=průměrná samostatnost,*** *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:

S tématem byl student obeznámen dlouho a v září 2017 o něm přednesl příspěvek na studentské konferenci STIGMA pořádané KTI. Přesto praktická část práce a text BP vznikaly ve spěchu před termínem odevzdání což se na nich silně podepsalo. Student navštěvoval dohodnuté konzultace a přinášel vlastní nápady, které mohly práci velmi obohatit, pokud by se povedlo je realizovat.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*45 (F)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Implementace algoritmů byla úspěšně dokončena, ovšem rozsah testování by bylo třeba rozšířit. Práci v současném stavu považuji za nedokončenou, zejména co se týče textu práce. Ten by potřeboval doznat zásadních změn, aby byl text konzistentní, srozumitelný a aby výsledky mohly být správně interpretovány. Po sjednocení značení, vysvětlení problematických míst v rešerši a doplnění komentářů ke zkoumaným algoritmům může být výsledná práce velmi kvalitní.

Podpis vedoucího práce: