FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Mgr. Martin Jureček, Ph.D.
Student:	Bc. Jan Dolejš
Název práce:	Algebraická kryptoanalýza zmenšených variant proudové šifry E0
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	5. února 2024

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Všechny body ze zadání práce považuji za splněné.

2. Písemná část práce 93 /100 (A)

Práce je dobře členěná, má odpovídající rozsah a seznam literatury obsahuje jen relevantní práce. Teoretická část obsahuje všechny pojmy a tvrzení potřebné k pochopení algebraické kryptoanalýzy šifry E0.
Student průběžně pracoval na jednotlivých kapitolách, proto bylo dost času na opravu chyb a jejich vylepšení. Na poslední chvíli byla přidána kapitola o LSH, která nebyla zkontrolována vedoucím práce a ve které se vyskytlo pár drobných překlepů:
- str. 24 poslední odstavec - "The MinHashing step uses m random permutations whose sizes equal the number of unique polynomials in the polynomial system." - velikost permutace by se měla rovnat počtu různých monomů a ne polynomů
- str. 26 - "...bucket with two two items,..." - objevuje sa 2x "two"
- str. 26, poslední odstavec - smysl thresholdu t mohl být lépe vysvětlen
Celkově hodnotím text práce za výborný.

3. Nepísemná část, přílohy 97 /100 (A)

Generování rovnic bylo naimplementováno v jazyce Python a pro výpočet Groebnerových bází se využil software Magma. Zpracování rovnic pomocí LSH navazuje na dvě práce předchozích studentů. Součástí práce je uživatelská dokumentace, na jejímž základě nebude složité použít studentův kód v navazujících pracích.

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Práce studenta přispěla k rozšíření kryptoanalýzy šifry E0 a vzhledem k dosaženým výsledkům má tato práce potenciál k publikaci.

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student pravidelně konzultoval s vedoucím práce nejnovější výsledky a další kroky po celou dobu práce.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Student si samostatně nastudoval potřebnou teorii a naimplementoval skripty provádějící generování rovnic a algebraickou kryptoanalýzu zjednodušených verzí šifry E0.

Celkové hodnocení 96 /100 (A)

Student navrhl zmenšené verze šifry E0 a převedl je na soustavu polynomiálních rovnic nad GF(2). Dalším přínosem je kapitola 2.2.5, kde student sám navrhl generování dalších rovnic. Na výslednou soustavu pak aplikoval algebraickou kryptoanalýzu a podařilo se mu prolomit 20-bitovou verzi šifry. Celý postup spolu s výsledky jsou pěkně zpracovány bez většího množství chyb. Z těchto důvodů navrhuji známku A.

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Aktivita studenta

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.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

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.