FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Mgr. Martin Jureček, Ph.D.
Student:	Bc. Daniel Minarovič
Název práce:	Algebraická kryptoanalýza zjednodušených variant šifry Grain-128AEAD
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	5. června 2023

Hodnotící kritéria

1. Splnění zadání

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

Všetky body zo zadania práce považujem za splnené.

2. Písemná část práce 58 / 100 (E)

Práca je dobre členená, má odpovedajúci rozsah a zoznam literatúry obsahuje len relevantné práce. Teoretická časť obsahuje všetky pojmy a tvrdenia potrebné k pochopeniu algebraickej kryptoanalýzy šifry Grain. Niektoré časti práce sú preložené z knihy bez doplňujúcich poznámok. Študent mohol doplniť viac príkladov podporujúcich teoretický výklad. Taktiež mohol byť kladený väčší dôraz na detailné definovanie zjednodušenej verzie šifry Grain. Túto časť práce považujem za najslabšiu. Napriek viacnásobnému upozorneniu študent pri zmenšení LFSR neponechal charakteristický polynóm primitívnym, čo je závažná chyba. Na druhej strane kladne hodnotím redukciu polynómov pomocou LSH techniky, ktorá bola nad rámec zadania.

3. Nepísemná část, přílohy 75 / 100 (C)

Generovanie rovníc bolo naimplementované v jazyku Python a na výpočet Groebnerových báz sa využil software Magma. Spracovanie rovníc nadväzuje na prácu študentky Jany Beruškovej. Súčasťou práce je užívateľská dokumentácia, na základe ktorej nebude zložité použiť študentov kód v nadväzujúcich prácach.

4. Hodnocení výsledků, jejich využitelnost 55 /100 (E)

Algebraická kryptoanalýza má uplatnenie pri analýze bezpečnosti šifier. Vzhľadom k aktuálne prebiehajúcej súťaži Lightweight Cryptography od NISTu, v ktorej sa Grain účastní finálového kola, by študentove výsledky mohli byť zaujímavé za podmienky, že by správne definoval zmenšenú verziu šifry.

5. Aktivita studenta

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

Študent konzultoval s vedúcim práce najnovšie výsledky a ďalšie kroky počas celého obdobia práce.

6. Samostatnost studenta

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

Študent si samostatne naštudoval potrebnú teóriu a naimplementoval skripty vykonávajúce algebraickú kryptoanalýzu zjednodušených verzií šifry Grain.

Celkové hodnocení 60 /100 (D)

Celkovo hodnotím prácu známkou D. Slabšou časťou práce je popis zmenšených verzií šifry Grain. Niektoré detaily neboli lepšie vysvetlené, pretože ani sami autori šifry Grain ich nevysvetlili v dokumentácii, avšak na obhajobe by študent mal presne definovať zmenšenú verziu Grainu a taktiež prezentovať výsledky, kde u zmenšeného LFSR bol použitý primitívny polynóm.

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.