FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Róbert Lórencz, CSc.
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 zadání byly splněny bez výhrad.

2. Písemná část práce 95 / 100 (A)

Práce má standartní strukturu. Rozsah práce je odpovídající obsahu. Kapitoly, které se věnují teorii, obsahují a vysvětlují odpovídající matematické pojmy a definice potřebné pro pochopení problematiky, kterou se práce zabývá. Student analyzoval vnitřní fungování šifry E0 a navrhl malé varianty šifry využívající lineární zpětnovazebné posuvné registry. V ostatních částech práce se student zabýval implementací, experimentům a analýze výsledků.

3. Nepísemná část, přílohy 96 / 100 (A)

Nepísemná část práce obsahuje implementace potřebných nástrojů v Jazyce Python pro provádění experimentů. Implementované nástroje jsou funkční a náležitě zdokumentované.

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

Práce je zdařilá, obsahuje zajímavé výsledky a myšlenky a má publikační potenciál.

Celkové hodnocení

96 /100 (A)

Práce se zabývá kryptoanalýzou zmenšené verze proudové šifry E0. Výsledky práce spočívají v návrhu soustav polynomiálních rovnic a jejich řešení pomocí řešičů F4 a SAT. Studentovi se podařilo dosáhnout zajímavých výsledků při řešení těchto rovnic a to konkrétně výrazného zkrácení času výpočtu. Práce má publikační potenciál.

Otázky k obhajobě

1. Je množina řešení pomocí Groebnerových bází stejná jako množina řešení pomocí SAT solveru? Zdůvodněte.
2. Ohledně tabulky 4.3, proč je minimální počet bitů potřebný k nalezení právě jednoho řešení stejný pro F4 algoritmus i pro SAT řešič?
3. Podle tabulky 4.4 se s rostoucím počtem bitů keystreamu výsledky F4 algoritmu zlepšují a naopak výsledky SAT řešiče se zhoršují. Proč tomu tak je?

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.

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.