FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Róbert Lórencz, CSc.
Student:	Bc. Jiří Soukup
Název práce:	Algebraická kryptoanalýza proudových šifer založených na LFSR
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	30. května 2022

Hodnotící kritéria

1. Splnění zadání

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

Zadáni bylo splněno ve všech bodech.

2. Písemná část práce 96 / 100 (A)

Práce má odpovídající členění dle zadání a požadavků na závěrečnou práci. Počet zdrojů a jejich volba je v souladu s obsahem práce. Popis algoritmů je příkladně zpracován a vysvětlen.

3. Nepísemná část, přílohy 99 / 100 (A)

Praktické provedení navrhovaných algoritmů bylo provedené v jazyku Python a pro výpočty byl využit katederní klastr se software Magma. Práce obsahuje uživatelskou příručku pro usnadnění použití software v dalším výzkumu.

4. Hodnocení výsledků, jejich využitelnost 98 / 100 (A)

Výsledky práce mají využití jak edukační tak rovněž pro další výzkum. Študent provedl prolomení 72 bitového generátoru, který obsahuje vyváženou boolevsku šifru.

Celkové hodnocení

98 /100 (A)

Práce je zdařila a její výsledky lze bezprostředně použít jako východisko pro další výzkum. Rovněž textová část obsahující teoretický výklad je použitelná jako edukační základ při řešení dalších závěrečných prací podobného charakteru.

Otázky k obhajobě

1. Jak by se změnily výsledky algebraické kryptoanalýzy n-bitové proudové šifry, pokud bychom měli k dispozici až 2n bitů keystreamu?
2. Proč se podařilo prolomit filtr generátor s větším vnitřním stavem než měl kombinační generátor?
3. Jak dále by se dala rozšířit vaše práce?

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.