FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Róbert Lórencz, CSc.
Student:	Bc. Jana Berušková
Název práce:	Redukování předefinovaných systémů polynomiálních rovnic odvozených ze zjednodušených variant AES
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	6. února 2023

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno bez výhrad.

2. Písemná část práce 88 /100 (B)

Práce je rozumně členěná. Rozsahem výraznější část práce tvoří úvodní kapitoly pojednávající o matematických základech Groebnerových bázích a popisu struktury šifry AES. Diplomantka navazuje na práci Mareka Bielika a její práce je hodně na tuto práci odkazována.

3. Nepísemná část, přílohy 92 /100 (A)

Diplomantka jak již bylo výše zmíněno vycházela z práce M. Bielika a to i v případě skriptů z této práce, které rozšířila a upravila. Výpočty prováděla s využitím funkcionalit software Magma.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Výsledky práce mají publikační potenciál. Jsou přínosné pro komunitu kryptoanalytiků zabývající se odolnosti AES vůči různým variantám útoků i kryptoanalýze.

Celkové hodnocení

91 /100 (A)

Práce je dobrým pokračováním DP M. Bielika. Diplomantka rozšířila metody generování rovnic, které vedli k lepším výsledkům, než práce, ze které vycházela. Její přínos je hlavně v zrychlení výpočtů rovnic v Groebnerových bázích. Diplomantka dosáhla toho zejména použitím tzv. metod shlukové analýzy (klastrování).

Otázky k obhajobě

Při práci s polynomy vznikl problém s nedostatkem paměti. Jak by se tento nedostatek mohl obejít? Např. za cenu zvýšení času výpočtu.
V experimentální části jste pokračovala i po odevzdání diplomové práce. K jakým dalším výsledkům jste se dopracovala?
Jakým směrem by se vaše práce mohla v budoucnu rozšířit?

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.