**FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE**

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Róbert Lórencz, CSc.
Student:	Bc. Marek Bielik
Název práce:	Algebraická kryptoanalýza zmenšených verzí šifry AES
Obor / specializace:	Systémové programování
Vytvořeno dne:	28. května 2021

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. Diplomant splnil všechny body zadání.

2. Písemná část práce — 92/100 (A)

Práce obsahuje všechny částí, které jsou vyžadované u ZP. Obsahově má práce těžiště zejména ve výkladové částí, kde diplomant opakuje znalosti potřebné k řešení zadání DP. Naopak část experimentální a část popisující řešení kryptoanalýzy AES variant je chudší. Určitě by zvýšení kvality práce prospělo tento poměr obrátit. Zdroje uvedené v práci odpovídají obsahu.

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

Řešení problému pomocí Gröbnerových bází a jiné experimenty byly vykonané v jazyku Python. Pro řešení polynomiálních rovnic byly použity Magma a CryptoMiniSat.

4. Hodnocení výsledků, jejich využitelnost — 99/100 (A)

Výsledky diplomanta jsou na velmi dobré úrovní a dokazují schopnost diplomanta řešit netriviální problémy z oblasti kryptoanalýzy šifer. Výsledky po doplnění experimentální části je možné publikovat.

Celkové hodnocení

98 /100 (A)

Práce diplomanta je na výborné úrovni. Je po úpravách a doplnění o další experimenty publikovatelná. Malé výhrady k práci se týkají struktury obsahu, kde je prostor na vylepšení v podobě podrobnějšího a názornějšího výkladu diplomantova přístupu a popisu experimentů.

Otázky k obhajobě

1) Jakým způsobem byste navrhl efektivnější způsob metody "guess and determine", než ten který byl použit v diplomové práci?
2) Jak byste navrhl použití metod strojového učení v případě kryptoanalýzy, která byla prezentovaná v práci?
3) Má diplomant představu kombinovaného přístupu založeného na použití metod uvedených v diplomové práci s lineární případně diferenciální kryptoanalýzou?

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. 26/2017, 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.