

Posudek oponenta závěrečné práce

České vysoké učení technické v Praze

Fakulta informačních technologií

Student: Bc. Jakub Tomanek
Oponent práce: prof. Ing. Róbert Lórencz CSc.
Název práce: Diferenciální kryptoanalýza šifry Baby Rijndael
Obor: Počítačová bezpečnost

Datum vytvoření: 7. 6. 2017

Hodnotící kritérium:	Způsob hodnocení - následující škálou 1 až 5:
1. Náročnost a další komentář k zadání	1=mimořádně náročné zadání, 2=náročnější zadání, 3=průměrně náročné zadání, 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání
Popis kritéria: Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)	
Komentář: Zadání vyžaduje teoretickou a praktickou znalost diferenciální kryptoanalýzy a znalost matematických principů šifer AES a Baby Rijndael. Zadání je rovněž náročné z hlediska realizace experimentů a jejich vyhodnocení.	
Hodnotící kritérium:	Způsob hodnocení - následující škálou 1 až 4:
2. Splnění zadání	1=zadání splněno, 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno
Popis kritéria: Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.	
Komentář: Zadání bylo splněno bez výhrad.	
Hodnotící kritérium:	Způsob hodnocení - následující škálou 1 až 4:
3. Rozsah písemné zprávy	1=splňuje požadavky, 2=splňuje požadavky s menšími výhradami, 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky
Popis kritéria: Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.	
Komentář: Rozsah práce splňuje požadavky na diplomovou práci.	
Hodnotící kritérium:	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):
4. Věcná a logická úroveň práce	98 (A)
Popis kritéria: 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.	
Komentář: Práce má jasnou logickou strukturu. Výklad obsahu v jednotlivých kapitolách je přehledný logicky strukturován. Výsledky experimentů jsou přehledně uvedené v tabulkách a grafech, které jsou příkladným způsobem okomentovány a textu práce důkladně diskutovány. Výskyt překlepů je minimální.	
Hodnotící kritérium:	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):
5. Formální úroveň práce	94 (A)
Popis kritéria: Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.	
Komentář: Práce má příkladnou formální úroveň. Výskyt překlepů je minimální.	
Hodnotící kritérium:	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):
6. Práce se zdroji	92 (A)
Popis kritéria: Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.	

Komentář:

Práce se zdroji odpovídá tématu a rozsahu práce.

Hodnotící kritérium:

Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):

7. Hodnocení výsledků, publikační výstupy a ocenění

96 (A)

Popis kritéria:

Vyjádrte se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:

Práce přináší zajímavý pohled na problematiku diferenciální kryptoanalýzy šifry Baby Rijndael. Precizní způsob zpracování experimentálních výsledků je příkladný. Rovněž pečlivý návrh a provedení jednotlivých variací vybrané kryptoanalytické metody na danou šifru je vzorový.

Hodnotící kritérium:

Způsob hodnocení - nehodnotí se

8. Komentář o využitelnosti výsledků

Popis kritéria:

Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:

Výsledky provedených kryptoanalytických experimentů založených na variacích diferenciální kryptoanalýzy Baby AES jsou inspirující a mohou být rozumným základem pro pokračování v tomto výzkumu. Z pohledu náročnosti zvoleného tématu jsou výsledky velmi pěkné, i když nepřináší pro praxi použitelné kryptoanalytické metody.

Hodnotící kritérium:

Způsob hodnocení - nehodnotí se

9. Otázky k obhajobě

Popis kritéria:

Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

Na závěr kapitoly 6 uvádíte srovnání výsledků dosažené ve Vaší práci s výsledky dosažené v jiných pracích. Máte návrh nebo doporučení pro nějakou hybridní metodu, která by kombinovala Váš přístup s přístupy uvedenými v jiných pracích, tak aby v konečném důsledku bylo dosaženo lepších výsledků kryptoanalýzy?

Hodnotící kritérium:

Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):

10. Celkové hodnocení

98 (A)

Popis kritéria:

Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:

Práce je velmi vydařená. Autor prezentuje hlubokou znalost řešené problematiky. Práce prezentuje tematicky komplexní a implementačně náročnější výzkumný projekt.

Podpis oponenta práce: