# Posudek oponenta závěrečné práce

**České vysoké učení technické v Praze** **Fakulta informačních technologií**

**Student:** Bc. Peter Poljak
**Oponent práce:** prof. Ing. Róbert Lórencz, CSc.
**Název práce:** The Impossible Differential Cryptanalysis
**Obor:** Počítačová bezpečnost

**Datum vytvoření:** 26. 1. 2017

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 5:* |
|---|---|
| **1. Náročnost a další komentář k zadání** | *1=mimořádně náročné zadání,*<br>***2=náročnější zadání,***<br>*3=průměrně náročné zadání,*<br>*4=lehčí, ale ještě dostatečně náročné zadání,*<br>*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 i praktickou (implementační) znalost principu kryptoanalytických metod.

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 4:* |
|---|---|
| **2. Splnění zadání** | ***1=zadání splněno,***<br>*2=zadání splněno s menšími výhradami,*<br>*3=zadání splněno s většími výhradami,*<br>*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,***<br>*2=splňuje požadavky s menšími výhradami,*<br>*3=splňuje požadavky s většími výhradami,*<br>*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 splňuje požadavky.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **4. Věcná a logická úroveň práce** | *78 (C)* |

*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 po věcné stránce nevykazuje zásadní nedostatky. Autorovi lze vytknout struktura a obsah 2. kapitoly, kde uvádí bez náležitého odůvodnění a velmi zevrubně lineární, diferenciální a algebraickou kryptoanalýzu. V práci chybí kapitoly pojednávající o implementační aspektech provedeného útoku na šifru Baby AES, chybí popis experimentu a vyhodnocení získaných dat z experimentu.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **5. Formální úroveň práce** | *88 (B)* |

*Popis kritéria:*
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.

*Komentář:*
Po formální stránce je práce dobře napsaná.Výskyt nepřesností a logických chyb je minimální.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **6. Práce se zdroji** | *88 (B)* |

*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 je vyhovující.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **7. Hodnocení výsledků, publikační výstupy a ocenění** | *88 (B)* |

*Popis kritéria:*
Vyjádřete 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:*
Výstupy práce mají standardní úroveň.

| *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:*
Dosažené výsledky v předkládané práci mohou být dobrým základem pro vytvoření výukových materiálů pro oborový předmět Pokročila kryptologie mag. oboru Bezpečnost na FIT.

| *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:*
1. Můžete u obhajoby uvést a vysvětlit obecný vztah pro prostorovou a časovou složitost provedeného útoku?
2. Můžete u obhajoby představit detailněji výsledky z provedeného experimentu?
3. Jaký je rozdíl mezi variantou 1 a 2 v kapitole 4.9.1 a 4.9.2?

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **10. Celkové hodnocení** | *87 (B)* |

*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 vcelku vydařená. Autor prezentuje dobrou znalost řešené problematiky. Po věcné a logické stránce má práce některé nedostatky (viz bod 4 tohoto posudku).

Podpis oponenta práce: