Posudek oponenta závěrečné práce

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

Student: Ondřej Semrád
Oponent práce: Ing. Vojtěch Miškovský
Název práce: Útok rozdílovou odběrovou analýzou na implementaci algoritmu AES na platformě Xilinx
Obor: Počítačové inženýrství

Datum vytvoření: 9. 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:
Tato práce navazuje na dřívější práce věnující se rozdílové odběrové analýze a dále na práci věnující se spolehlivostním variantám šifry AES. Ačkoli byla nemalá část implementace převzata z těchto prací, autor musel pro splnění zadání skloubit znalosti návrhu hardware i software a také další znalosti vyučované až v magisterském studiu. Proto považuji zadání za nadprůměrně náročné.

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 bez výhrad splněno.

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 je vysoce nadprůměrný. Práce je informačně bohatá. Popis implementace AES je možná až příliš podrobný.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*85 (B)*

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:
Ačkoli celkově je věcná i logická úroveň práce nadprůměrná, musím zmínit i několik nedostatků.
1) Poslední dva odstavce úvodu jsou informačně velmi podobné a působí dojmem, že autor jeden z nich zapomněl smazat.
2) V sekci 4.2.1.1 mi přišel popis použitého modelu spotřeby velmi zmatečně popsaný.
3) Při hledání nejmenšího počtu potřebných průběhů při použití časové redundance (sekce 4.2.3.5 a 4.2.3.6) mi přijde nevhodné zaměřit se pouze na jeden vzorek, neboť korelační extrémy se dají očekávat ve třech vzorcích.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*70 (C)*

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:
Jazyková úroveň práce je nadprůměrná, nicméně občas jsem narazil na sémanticky zvláštní souvětí. Také se v práci objevují výrazy nevhodné pro odborný text (přixorovat, natvrdo zadrátovat klíč). V několika nadpisech čtvrté kapitoly se objevuje výraz "DPA na čipovou kartu" (správně spíše DPA na čipové kartě, nebo DPA pro čipovou kartu).
Dále se mi z formálního hlediska nelíbilo:
- příliš dlouhé popisy obrázků (v některých případech by stačilo použít alternativní popis jen pro účely seznamu obrázků, jinde by bylo vhodnější celý popisek zkrátit a informace podat v textu)
- místy nedostatečné členění textu do odstavců
- neoddělování odkazů na literaturu mezerou
- nevhodně zvolený rozsah osy Y v obrázku 1.8 (obrázek je tudíž špatně čitelný)
- kombinování prostředí equation a figure (obrázky 1.6 a 1.7)
Celkově hodnotím formální úroveň práce jako lehce nadprůměrnou

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*95 (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:
Autor využívá relevantní zdroje, korektně je cituje a jejich výsledky jasně odděluje od vlastních.

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

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:
Tato práce je součástí rozsáhlejšího výzkumu na KČN. Autorova implementace i výsledky budou použity pro další výzkum.

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 jsou součástí širšího výzkumu, nicméně autorovy závěry mohou být již nyní uplatňovány v praxi.

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) V sekci 2.1 autor srovnává rychlost výpočtu korelací v programech MATLAB a Mathematica. Pracoval autor při výpočtech v Mathematice s nepřesnými čísly (pomocí funkce N)? Pokud ne, mohl by to napravit a provést srovnání znovu?
2) V tabulce 4.1 jsou vidět velké rozdíly mezi počty průběhů potřebnými pro získání jednotlivých bytů správného klíče. Dokázal by autor vysvětlit, co je jejich příčinou?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*83 (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:
Zadání práce je nadprůměrně náročné a využitelnost výsledků neoddiskutovatelná. Formální nedostatky bohužel sráží celkovou kvalitu práce. Práci doporučuji k obhajobě a hodnotím stupněm B.

Podpis oponenta práce: