Posudek oponenta závěrečné práce

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

Student: Jan Severyn
Oponent práce: Ing. Vojtěch Miškovský
Název práce: Útoky postranními kanály na implementace kryptografických algoritmů
Obor: Počítačové inženýrství

Datum vytvoření: 5. 1. 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:
Útok rozdílovou odběrovou analýzou je na FIT vyučován v magisterském předmětu MI-BHW, kde je prováděn na SmartCard. Provést tento útok na FPGA se v době odevzdání této bakalářské práce nedařilo ani zaměstnancům KČN. Pro samotné měření rozdílové analýzy odběru bylo třeba zvolit vhodnou vývojovou desku (a dokonce ji upravit), vytvořit implementaci v FPGA a vytvořit vhodné softwarové nástroje pro běh a vyhodnocení útoku. Bylo tedy zapotřebí skloubit široké spektrum znalostí. V tomto kontextu by bylo zadání náročné i pro diplomovou práci, hodnotím jej tedy jako mimořádně náročné i přes fakt, že na tématu autor spolupracoval s dalším studentem. Zkušenosti získané a prezentované v této práci budou využity pro další výzkum na KČN.

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:
Ačkoli se v rámci této práce nepodařilo na FPGA úspěšně provést útok, nelze to považovat za nesplnění zadání. Všechny dílčí kroky jsou náležitě zdokumentovány a autor nabízí i různá vysvětlení neúspěchu. I vzhledem k výše zmíněné náročnosti zadání tedy tento neúspěch hodnotím jako menší výhradu.

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:
Písemná zpráva se rozsahem blíží požadavkům na diplomovou práci (52 stran textu).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*87 (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:
Věcná a logická úroveň práce je na vysoké úrovni. Text je dobře uspořádaný, kapitoly plynule navazují, autor na vhodných místech odkazuje na související obsah z jiných kapitol. Průběh všech prací je dobře zdokumentovaný. Výtku bych měl k sekci 4.2, kde autor popisuje testování navržené VHDL implementace AES. Zmiňuje zde verifikaci pomocí simulace šifrovací části návrhu, nikoli však komunikační části návrhu, která by dle mého názoru měla být taktéž odsimulována. Případná chyba v této části návrhu by mohla být příčinou nestability při komunikaci přes USB-UART převodník, kterou autor v téže sekci popisuje. Dále v sekci 1.2, kde autor popisuje DPA, je zmíněno, že při DPA se využívá rozdílné spotřeby hradla či klopného obvodu při logické nule a jedničce, což rozhodně nelze obecně prohlásit. Celkově by popis DPA v této sekci mohl být trochu obecnější.

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 jazykové stránce je práce napsána velmi pěkně a dobře se čte. V textu jsem objevil přibližně 20 pravopisných chyb nebo překlepů, což je vzhledem k rozsahu práce přijatelné. Jedinou výjimkou je anglický abstrakt. Zde je jazyk dosti neobratný a chyb je zde na jeden odstavec příliš. Z typografického hlediska se mi nelíbilo zalamování názvů VHDL objektů a souborů na konci řádků (viz např. sekce 3.1 a 3.2.2). Dále by měl autor pro matematické výrazy využívat k tomu určené prostředí systému Latex a volit krátké značení proměnných a ty následně v textu definovat (viz sekce 3.1).

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 důležitá tvrzení podkládá relavantními citacemi. Vhodné části implementace jsou realizovány existujícími řešeními, o čemž autor informuje. Části realizované ve spolupráci s dalším studentem jsou jasně označeny. Použitá literatura je uvedena v souladu s citačními normami. Citovaná literatura obsahuje vhodnou kombinaci teoretických publikací a praktických poznatků. Její důležitou součástí jsou implementační práce vzniklé na FIT, na které autor plynule navazuje.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*85 (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:

Ačkoli práce nedosáhla zamýšleného výsledku, výstupem je velmi dobře zpracovaný popis neúspěchu, popis možností dalšího pokračování pro dosažení úspěšného útoku a prostředí pro jeho realizaci, které autor vytvořil.

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:

Zkušenosti získané při zpracování této práce byly a budou využity pro další zkoumání DPA na FPGA na FIT. Stejně tak hardwarová i softwarová část implementace budou moci být dále využívány.

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:

Pokračoval autor na této práci po odevzdání a dopracoval se k úspěšné realizaci útoku?
Pokud ano, dokázal by v práci identifikovat nějaké rozhodnutí, které mu bránilo v úspěšné realizaci?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*89 (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 bylo velmi náročné zejména s ohledem na velký rozsah potřebných znalostí, které často nejsou součástí bakalářského studia. Také časová náročnost implementace celého řešení pro realizaci DPA, stejně jako i samotného měření, je vysoká. Navíc i písemná zpráva je na poměry bakalářských prací poměrně kvalitní a rozsáhlá. Vzhledem k těmto okolnostem autorovi nelze příliš vyčítat, že se mu samotný útok na FPGA nepodařil, a práci hodnotím jako zdařilou. S ohledem na výtky u formální a věcné úrovně práce bych ji ocenil stupněm B, tedy velmi dobře.

Podpis oponenta práce: