Posudek oponenta závěrečné práce

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

Student: Martin Mašek
Oponent práce: Ing. Vojtěch Miškovský
Název práce: Vliv obrany hardwarové implementace AES vůči fault-injection útokům na její odolnost před útoky rozdílovou odběrovou analýzou
Obor: Počítačové inženýrství

Datum vytvoření: 6. 4. 2018

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 považuji za mimořádně náročné, neboť pro jeho splnění je třeba zkombinovat znalosti číslicového návrhu, statistického vyhodnocování, elektroniky a kryptografie.

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:
Student vytvořil implementaci šifry AES a jejích variant pro ochranu před fault-injection útoky v FPGA. Na všech variantách následně prováděl útok DPA a pokusil se porovnat, zda a případně jakým způsobem se liší náročnost DPA pro jednotlivé varianty. Z dosažených výsledků vyplývá, že jednotlivé ochrany se co do odolnosti proti DPA neliší, nicméně nebylo dosaženo srovnání s originální variantou bez ochrany, na které se studentovi nepodařilo útok provést. Tento dílčí neúspěch je s ohledem na náročnost zadání odpustitelný. Student nicméně v práci nijak nedokumentuje pokus o analýzu tohoto problému a nenaznačuje žádný postup pro jeho vyřešení. Pouze konstatuje, že "Zkoumané varianty neprojevily výraznější dopad na proveditelnost útoku diferenciální proudovou analýzou". Toto tvrzení, vzhledem k chybějícímu porovnání s nezabezpečenou variantou, považuji minimálně za odvážné.

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 písemné zprávy plně odpovídá bakalářské práci. Všechny části jsou informačně bohaté.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*92 (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:
Uspořádání práce je zcela v pořádku, práce je členěna logicky a dobře se čte. Drobnou výtku mám k první kapitole, kde práce obsahuje malé množství faktických nepřesností, zejména v části o útoky postranními kanály.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*95 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Komentář:
Formální úroveň práce je až na menší množství překlepů a několik neobratných vyjádření zcela v pořádku.

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 vycházel zejména z poznatků dřívějších studentů, nicméně své řešení porovnával i s relevantními mezinárodními publikacemi. Všechny zdroje odpovídajícím způsobem cituje. Celkově hodnotím práci se zdroji velmi pozitivně.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*75 (C)*

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:
Výsledky mají vysokou hodnotu, bohužel však nejsou kompletní.

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 rozšiřují dosavadní poznatky o vlivu ochran před fault-injection útoky na odolnost proti útokům postranními kanály.

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:
Nemám otázky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*80 (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 této práce bylo obtížné, přesto student zadané téma kvalitně zpracoval a zdokumentoval. Bohužel se však studentovi nepodařilo splnit důležitý bod zadání a ani se nepodařilo tento neúspěch relevantně odůvodnit. Nicméně vzhledem ke zmíněné obtížnosti a kvalitě zpracování tématu hodnotím celkově práci stupněm B a doporučuji k obhajobě.

Podpis oponenta práce: