FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

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

Datum vytvoření: 14. 6. 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 je náročnější, protože spojuje několik různých disciplín (číslicový návrh, spolehlivost, statistiku, elektroniku). Autor měl však výhodu, že se podobnými tématy na stejné nebo podobné desce zabývali již čtyři jeho předchůdci, měl tedy na koho navazovat.

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:
Autor naimplementoval základní variantu AES a 5 různých variant s obranami proti fault-injection útokům, tak jak byly posány v [16]. Vynechal pouze obvod pro výpočet zbytku po dělení 7mi (modulo 7). Na všech 6 variant (1 základní a 5 s ochranami) poté aplikoval DPA. Zajímavé je, že se mu nepodařilo vůbec prolomit základní variantu. Schází mi diskuse tohoto jevu. Ostatních pět variant prolomil bez problémů.

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:
Autor re-implementoval struktury popsané v literatuře [16]. Toto však není v textu dostatečně zdůrazněné, respektive v sekci 1.5 se zmiňuje i o literatuře [15], z níž ale zřejmě nebyla použita žádná struktura. Autoři [16] implementovali svoje struktury pro ASIC a odolnost těchto struktur vůči DPA byla následně zkoumána simulací, přičemž simulovali pouze SBox se zabepečujícími sktrukturami, nikoliv AES jako celek. Oproti tomu autor BP implementoval celý AES, na FPGA, a spotřebu obvodu nesimuloval, ale změřil spotřebu skutečného reálného obvodu. Toto by mělo být zdůrazněno v práci. Rovněž bych přivítal srovnání závěrů studie [16] se závěry této bakalářské práce.

Tabulka 5.6 měla být doporovozena krabicovým grafem (BoxPlot), abychom mohli zkoumat, zda se mezikvartilové intervaly překrývají, a jak.

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

4. Věcná a logická úroveň práce	*95 (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:
Nerozumím tomu, proč je v obvodu pro AES (obrázek 3.4) použit výstupní registr (OUTPUT_REG). Ciphertext lze číst přímo z výstupu ROUND_REG.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*60 (D)*

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:
- Autor zavádí nový pojem Diferenciální proudová analýza, čímž se rozumí Rozdílová odběrová analýza.
- Nemá popsané osy grafů (např. 5.1), případně je má popsané chybně (obr. 5.2 korelace -> korelační koeficient).
- V popisku grafu 5.1 píše "vzorek spotřeby" namísto "průběh spotřeby".
- V sekci 1.5 zmatečně popisuje použité ochrany proti fault-injection útokům (například popis sudé/liché parity).
- Sekce 3.1.2.1 postrádá jakýkoliv úvod (že následující text popisuje jednotlivé stavy konečného automatu pro přijímání dat; že graf tohoto automatu je na obrázku 3.2., a že tento automat je uvnitř jednotky COMMUNICATOR). Toto vše si musí čtenář domyslet. Totéž se opakuje o sekci dál.
- V sekci 3.1.2 není jasné, jak se rozliší zaslaný klíč a data. Až později se čtenář z textu musí dovtípit, že pro zaslání nového klíče je nutné stisknut tlačítko RESET (které je to tlačítko na desce?). Za klíč se považují první zaslaná data po resetu.
- Sekce 3.2.5 je nesrozumitelná.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*85 (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:
Autor nastudoval poměrně velké množství literatury. Přivítal bych větší provázanost jeho textu s nastudovanou literaturou, například srovnání jeho výsledků s výsledky v [16].

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:
Autorovi se bohužel nepovedlo provést útok na základní variantu AES. Vzhledem k tomu, že tuto variantu již na našem pracovišti prolomit umíme, měl konzultovat svoje problémy s vedoucím práce nebo se svými úspěšnějšími kolegy.

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:
VHDL kódy vytvořené autorem můžeme použít a případně zopakovat měření, abychom je mohli přičlenit ke stávající sadě struktur, které máme k dispozici (prostorová a časová redundance).

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* ***3=průměrná aktivita,*** *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: *1=výborná samostatnost,* ***2=velmi dobrá samostatnost,*** *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Autor začal na bakalářské práci pracovat již na jaře 2016. V té době byl poměrně aktivní. Následně ale přerušil studium a po ukončení přerušení jsme téma bakalářky museli upravit, protože původní téma již bylo vyřešeno jinými autory. Vzhledem k časovému vytížení autora se poté již konzultace konaly velmi sporadicky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*75 (C)*

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:
Pokud by autor nebyl pod časovým tlakem, jistě by se mu podařilo odstranit problém z kryptoanalýzou základní verze AES. Rovněž pravidlené konzultace s vedoucím práce by přispěly k vyšší kvalitě textu.

Podpis vedoucího práce: