Posudek oponenta závěrečné práce

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

Student: Bc. Lukáš Mazur
Oponent práce: Ing. Vojtěch Miškovský
Název práce: Side channel analysis of cryptographic algorithms implementations
Obor: Počítačové inženýrství

Datum vytvoření: 24. 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:
Útoky postranními kanály se na FITu vyučují až v magisterském studiu, konkrétně je prováděna rozdílová odběrová analýza na SmartCard. Útok na FPGA je daleko náročnější a jeho implementace vyžaduje široké spektrum znalostí v oblasti hardware i software. Útok samotný je také časově náročný. Zadání bych považoval za náročné i pro diplomovou práci, v případě bakalářské práce jej tedy hodnotím jako mimořádně náročné, i když autor částečně spolupracoval s dalším studentem. Výsledky práce budou dále využívány pro 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:
Zadání bylo splněno. Autor úspěšně získal šifrovací klíč ze šifrovacího zařízení implementovaného v FPGA a prozkoumal vliv různých variant měření a implementace na proveditelnost útoku.

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 bohatě překonává i podmínky pro diplomovou práci. Obsah je vyvážený a informačně hodnotný.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*90 (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:
Věcná a logická úroveň je vysoká. Text se dobře čte, plynule navazuje. Autor vhodně odkazuje na související obsah z jiných částí práce. Práce obsahuje podrobný popis všech částí implementace i naměřených výsledků. Pouze bych vytkl, že v kapitole 4 o testování autor zmiňuje simulaci VHDL kódu, ovšem pouze samotného šifrovacího modulu AES. Zde by měl autor odsimulovat všechny části VHDL implementace. Drobnou výtku mám také k první kapitole. Konkrétně k části 1.2.1, kde autor popisuje rozdílovou odběrovou analýzu pouze konkrétně na šifře AES. Zde by bylo vhodnější ji popsat obecně a až poté demonstrovat na AES.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*98 (A)*

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:
Formálně je práce na velmi vysoké úrovni. Autor velmi dobře využívá a kombinuje dostupné prostředky (textový popis, obrázky, tabulky, poznámky pod čarou...). Práce je psána v anglickém jazyce, což oceňuji. Jazyková úroveň je vysoce nadprůměrná, nenašel jsem žádné závažné pravopisné chyby či překlepy, pouze minimální množství chybějících členů. Po typografické stránce je práce také kvalitní. Pouze bych doporučil používat vhodnější zápis rozměrů matic (viz sekce 3.2).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*97 (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:
Práce se zdroji je kvalitativně i kvantitativně vynikající. Seznam zdrojů odpovídá normám a všechny zdroje jsou citovány v souladu s citační etikou. Pouze u tvrzení v sekci 2.2.1, že Hammingova vzdálenost je vhodnější pro model spotřeby v FPGA než Hammingova váha, mi chybělo podložení relavantní literaturou.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*95 (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:
Výstupy odpovídají očekávání. Autor úspěšně provedl útok rozdílovou odběrovou analýzou na vývojové desce Spartan 3E Starter Board, kvalitně popsal svůj postup a zhodnotil složitost útoku pro různé varianty měření.

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:
Možnost provádět útok rozdílovou odběrovou analýzou na desce Spartan 3E Starter Board bude využita pro výzkum na KČN. Autor rozšířil portfolio platforem, na kterých můžeme útok provádět, a tedy rozšířil možnosti porovnávání a ověřování výsledků výzkumu.

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:
V sekci 5.2 autor uvádí, že naměření 100 000 průběhů trvá přibližně dvě hodiny a že úzkým hrdlem je zde přenos po sériové lince. Při rychlosti 115 200 baud/s a 17+16 přenesených bytech na jedno měření však vychází doba přenosu dat pro jeden průběh na 10*33/115200 s, tedy přibližně 3 ms a tudíž asi 5 minut při 100 000 průběhů. Dokázal by autor lépe identifikovat slabinu, která způsobuje takto dlouhé měření průběhů?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*97 (A)*

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:
Splněním zadání autor prokázal komplexní schopnosti. Rozsah provedených prací a písemné zprávy odpovídá spíše diplomové práci. Kvalita prací i zprávy je vysoce nadprůměrná, což je ještě podtrženo velmi solidní úrovní anglického jazyka, v němž je zpráva napsána. Využitelnost výsledků je nezpochybnitelná. I přes drobné výtky tedy práci nemůžu hodnotit jinak než výborně, tedy stupněm A.

Podpis oponenta práce: