FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Tomáš Balihar
Oponent práce:	Ing. Vojtěch Miškovský, Ph.D.
Název práce:	Influence of Synthesis Parameters on Vulnerability to Side-Channel Attacks
Obor:	Návrh a programování vestavných systémů

Datum vytvoření: 21. 8. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. 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 dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Zadání považuji za průměrně náročné a bylo studentem bez výhrad splněno.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*75 (C)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Rozsahově je text spíše kratší, nicméně informačně dostatečně bohatý. K obsahu mám větší výhradu pouze u analytické/rešeršní kapitoly. Očekával bych trochu širší přehled o útocích postranními kanály. Dále bych ocenil ucelenější přehled o diplomové práci, na kterou autor navazuje, neboť informace o ní jsou rozkouskované po celém textu. Ve druhé kapitole bych pak ocenil shrnutí obsahu celého navrženého experimentu do tabulky. Celkově je ovšem text logicky členěný a dobře pochopitelný. Oceňuji, že student psal práci v anglickém jazyce, a i přes občasné chyby či neobratné větné konstrukce považuji jazykovou úroveň za nadprůměrnou. Poměrně matoucí typografickou chybu v rovnici 1.1 ("S mínus box") či chybějící autorem zadefinové zkratky v seznamu zkratek považuji za drobné nedostatky, větší výhrady mám ke grafům. Snad ve všech grafech jsou prakticky nečitelné popisky os a hodnoty. Linie znázorňující jednotlivé rundy šifry jsou zbytečně výrazné a snižují čitelnost samotného obsahu grafů. Dále bych považoval za vhodné, aby grafy, u kterých se očekává přímé porovnávání (např. 1.7 (a) vs. (b), 3.4 vs. 3.5,...), měly shodné rozsahy os. Bibliografie je formálně v pořádku, nižší množství použité literatury souvisí s vytýkanou slabší rešeršní částí.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*90 (A)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:
Autor pro měření vytvořil plugin pro existující software a navrhl skripty pro vyhodnocení experimentu. Experiment byl dobře navržený, jeho výsledky jsou v práci srozumitelně a logicky shrnuté. Rozsah experimentu odpovídá zadání práce.

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

4. Hodnocení výsledků, jejich využitelnost — *80 (B)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Student navázal na výsledky dříve prezentované v jiné diplomové práci. Výsledky experimentů jsou přínosné, ovšem pro jejich vyšší statistickou relevanci by bylo třeba je ještě výrazně rozšířit. To nebylo možné vlivem velmi pomalého měření, které, jak je v práci vysvětleno, nešlo upravit, neboť by výsledky nebyly přímo porovnatelné s původní prací.

Hodnotící kritérium: — *Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

- V sekci 3.1 autor uvádí, že rozdílnost naměřených výsledků pro stejné bitstreamy mohla být způsobena rozdílnými fyzikálními podmínkami během měření. O jaké fyzikální podmínky se jedná a bylo možné tyto vlivy eliminovat?
- V obrázku 3.1 jsou vyznačeny linie rozdělující průběh spotřeby na jednotlivé rundy šifry. Očekával bych, že začátek rundy bude odpovídat náběžné hraně hodin prvního taktu rundy. Vzhledem k tomu, že na Sakura-G se měří úbytek napětí, spodní špičky spotřeby, kterými vyznačené linie prochází, by měly odpovídat lokálnímu maximu odebíraného proudu. To ovšem zřejmě neodpovídá náběžné hraně hodin. Jakým způsobem autor určoval počátek rundy? Jedná se o chybu, nebo má umístění vyznačených linií jiné vysvětlení?

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

6. Celkové hodnocení — *80 (B)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Student odvedl kvalitní práci. Rozsah experimentů mohl být větší, což však, jak vysvětluji výše, není přímo vina autora. V písemné zprávě postrádám trochu hlubší rešerši a mám výhrady k přiloženým grafům. I tak text považuji celkově za poměrně kvalitní i s přihlédnutím k tomu, že autor se rozhodl psát v angličtině. Práci doporučuji k obhajobě a navrhuji klasifikovat stupňem B.

Podpis oponenta práce: