FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Jan Brejník
Vedoucí: práce:	Ing. Stanislav Jeřábek
Název práce:	Obrany proti útokům postranními kanály založené na dynamické rekonfiguraci FPGA
Obor:	Návrh a programování vestavných systémů

Datum vytvoření: 29. 1. 2019

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:

Student splnil všechny body zadání a odvedl více práce, než bylo požadováno. Prostudoval možnosti využití dynamické rekonfigurace (dle zadání), kterých nejenom využil, ale navíc stvořil nástroj pro generování VHDL kódu s využitím technik dynamické rekonfigurace a dalších protiopatření uvedených v odkazované odborné literatuře. S využitím tohoto nástroje naimplementoval také AES (určený k prozkoumání možností) a provedl na všech implementacích dostatečný počet měření pro vyhodnocení (v zadání „alespoň několik pokusných“).
Pokud by všechna odvedená práce byla popsána v zadání, jednalo by se o zadání velmi obtížné a obsáhlé.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*95 (A)*

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:

Rozsah práce je bez příloh obsahujících přehled implementací a použitých útoků plných 100 stran. V textu nic nepřebývá, ani nechybí. Vše je popsáno dostatečně a v inovativní implementační části také návodně včetně specifikace použití nástroje pro generování VHDL kódu, který vznikl jako vedlejší produkt.
V práci se občas nachází drobné překlepy či záměna podstatných a přídavných jmen. I přes tyto chyby je však práce jasně srozumitelná a dobře čitelná. Jedinou drobnou výjimkou v tomto smyslu je Tabulka 2.2, kde je nesprávně jako typ atributu PortsCount uveden boolean, přičemž dle popisu atributu se jistě jedná o přirozené číslo.
Práce je věcně správná a ocitována v souladu s pravidly. Použita je především odborná literatura, dále pak u obecných témat (např. lineární transformace) výukové materiály a v jednom případě pro doplnění materiálů také anglrze wikipedie.

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

Součástí práce se SW pro generování kódu za použití v práci používaných ochran.
Provedená experimentální měření jsou snadno opakovatelná (včetně zapojení zdokumentovaného nejen textově, ale i formou fotografie s popisky). Dostatečně popsána je také metodika pro jejich vyhodnocení.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*100 (A)*

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:

Výsledky jsou kvalitní, inovativní a s publikačním potenciálem. Implementace šifry SERPENT je nová a doplňuje již publikované výsledky pro šifru PRESENT. V případě šifry AES jde pak také o výsledky nové a v případě použití konečných těles pak o řešení dosud nezkoumaných problémů.
Nástroj pro generování kódu, který vznikl jako vedlejší produkt, je v současnosti v recenzním řízení na mezinárodní konferenci DDECS 2019.

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

Popis kritéria:
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student byl aktivní a některé problémy konzultoval mj. se zahraničními odborníky (např. N. Mentens, viz str. 26).
Student pracoval samostatně a dobře. Posunutí původního termínu odevzdání je z převážné míry způsobeno konečnou rozsáhlostí celé práce.

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

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 splnil všechny body zadání a odvedl více práce, než bylo požadováno. Výsledky jsou kvalitní a s publikačním potenciálem.
Pokud by všechna odvedená práce byla popsána v zadání, jednalo by se o zadání velmi obtížné a obsáhlé.
Student navíc stvořil nástroj pro generování VHDL kódu s využitím technik dynamické rekonfigurace a dalších protiopatření uvedených v odkazované odborné literatuře, který byl odeslán k publikaci na mezinárodní konferenci (nyní v recenzním řízení).

Podpis vedoucího práce: