FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Petr Moucha
Oponent práce:	Ing. Stanislav Jeřábek
Název práce:	Ochrana šifry PRESENT prostřednictvím falešných a vícenásobnýcch rund na FPGA
Obor:	Počítačové inženýrství

Datum vytvoření: 27. 1. 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 bylo nejen ve všem splněno, ale výrazně překročeno. Autor znovuimplementoval šifru PRESENT se všemi dříve implementovanými i navrženými ochranami, ale také v rámci analýzy navrhl a později implementoval i vyhodnotil jím navržené nové ochrany. Jeho implementace i nové modifikace navíc vykazují výsledky vysoce převyšujícíc očekávání.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*99 (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:
Práce je napsaná přehledně a čtivě. V práci jsem nenašel jedinou hrubku, překlep či typografickou chybu. V tištěné verzi jsou jen nesprávně na výšku str. 13 a 39 obsahující obrázky na šířku. Jde však o chybu při tisku, v lektrnické verzi je toto správně. Jedinou nepřehlednost způsobuje tabulka 4.2 přes celou stránku vložená mezi položky nečíslovaného seznamu, což ovšem provedl sázecí nástroj.
Autor cituje 25 zdrojů, které jsou všechny relevantní.

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:
Autor implementoval všechny varianty obvodu ve VHDL. Následně naměřil jejich výsledky a vyhodnotil je.
Autor použil většinově nástroje převzaté. Jím vytvořený program pro generování konfigurací obvodu má širokou a přehlednou nabídku nastavení. Pozitivně oceňuji také jeho propojení s použitým nástrojem SICAK.

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 práce jsou vynikající. Nejen že je odveden velký kus práce, ale výsledky mají i vědeckou hodnotu. Plánujeme je publikovat na mezinárodní konferenci.

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:

1) Jsou podle vás vysoké hodnoty t-testu po konci šifrování na závadu nebo v pořádku? Proč?

2) Měřil jste některé scénáře vícekrát? Například porovnání scénářů 18 a 19 je překvapivé. Napadlo Vás od doby odevzdání práce, čím by to mohlo být?

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:

Zadání je ve všem splněno, výsledky jsou vynikající. Autor navíc v rámci analýzy navrhl další modifikace, které také naimplementoval, naměřil a zhodnotil jejich výsledky. Práce má vědecký přínos, který plánujeme publikovat. Doporučuji práci navrhnout na cenu děkana.

Podpis oponenta práce: