FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Kryštof Šádek
Oponent práce: Ing. Filip Kodýtek
Název práce: True random number generator on FPGA
Obor: Bezpečnost a informační technologie

Datum vytvoření: 15. 6. 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:
Student splnil zadání.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*90 (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 dobře strukturovaná a neobsahuje zbytečné části.
V sekci 2.3.4 by si popis NIST testu zasloužil více prostoru, aby bylo jasné jak vyhodnocení probíhá a co je pro to potřeba.
Kapitola 3 - běží všechny kruhové oscilátory v návrhu najednou během měření? Z obrázku 3.3 to tak vyplývá, ale není to nikde zmíněno. Pro testování TRNG by bylo vhodnější, aby byly povolené jen kruhové oscilátory, které jsou spolu v páru, aby se omezil jejich vzájemný vliv.
Kapitola 4 - nejasný popis obsahu histogramu na obrázku 4.1

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*95 (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:
Zdrojové kódy jsou přehledné a dobře komentované. Student jasně oddělil vlastní a převzatou práci.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*90 (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:
Student provedl měření pro vyhodnocení již navrženého TRNG na modernějším FPGA a provedl implementaci základních testů pro monitorování správné funkcionality daného TRNG za běhu. Práce je použitelná jako základ pro další zkoumání.

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: Na základě čeho byl vybrán kruhový oscilátor použitý pro vytvoření 4.1? Proč byl vybrán jen Frequency a Runs test? Zabýval se student i dalšími testy ze sady NIST? Bylo by vhodné některé z nich přidat? Tab 4.3 ukazuje selhání jednoho konkrétního páru kruhových oscilátorů. Byl tento pár nějak dále zkoumán pro zjištění příčiny tohoto chování?	
Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*90 (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: Práce byla dobře napsaná a strukturovaná. Kladně také hodnotím implementaci a prezentované výsledky. Práci hodnotím známkou A.	

Podpis oponenta práce: