FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Róbert Lórencz, CSc.
Student:	Tomáš Suda
Název práce:	Implementace a analýza TERO TRNG na FPGA
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	–

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Zadání bylo splněno bez výhrad.

2. Písemná část práce 97 /100 (A)

Práce rozsahem odpovídá řešeným tématům dle zadání. Obsah je dobře strukturovaný a přiměřený.. Pokrývá všechny důležité aspekty implementace a analýzy TERO-based TRNG na FPGA. Práce je věcně správná, bez patrných chyb nebo nepřesností.
Logická struktura práce je dobře promyšlená, kapitoly na sebe logicky navazují. Text je srozumitelný a dobře strukturovaný. Formální zápisy jsou správně používány, odborná terminologie je konzistentní. Typografická a jazyková stránka práce je na vysoké úrovni, bez gramatických chyb. Práce odpovídá akademickým standardům.
Student správně využil a citoval relevantní zdroje.

3. Nepísemná část, přílohy 98 /100 (A)

Nepísemná část práce odpovídá seznamu, který je v práci uveden. Všechen přiložený software je funkční.

4. Hodnocení výsledků, jejich využitelnost 98 /100 (A)

Implementace TRNG na FPGA umožňuje použití v kryptografických zařízeních pro generování skutečně náhodných čísel.
Vyvinuté skripty a nástroje mohou být použity pro rychlé testování a ověřování náhodnosti a bezpečnosti generátorů v praxi.

Práce představuje nové metody pro analýzu TERO-based TRNG, včetně automatizace testování a analýzy.
V práci autor zkoumá různé varianty implementaci a jejich vliv na výkon a bezpečnost., což přináší informace o optimálních konfiguracích.
Empirické testování různých konfigurací TRNG poskytuje nové poznatky o jejich výkonu a bezpečnosti v reálných podmínkách.

Celkové hodnocení

100 /100 (A)

Práce poskytuje důkladný přehled o generátorech náhodných čísel a jejich významu v kryptografii. Zejména je tady detailní popis TERO-based TRNG, jeho funkce a vlastností, včetně nových poznatků. Praktická část zaměřená na implementaci TRNG na FPGA je přehledná a dobře strukturována. Práce obsahuje podrobnou analýzu implementovaného TRNG, včetně měření a statistického vyhodnocení. Výsledky jsou jasně a srozumitelně prezentovány. Výsledky analýzy obsahují rovněž empirické testování různých konfigurací TRNG.
Závěrem můžu konstatovat, že práce je kvalitní a přináší nové poznatky. Rozšiřuje již publikované výsledky v oblasti TRNG, což může mít vliv na hardwarovou bezpečnost.

Otázky k obhajobě

Máte nějakou hypotézu o tom, proč se při výběru specifických prvků FPGA (LUT6_OR_MEM) choval navržený generátor lépe?.
Co se týče metodiky návrhu TERO buňky, vypozoroval jste nějaké závislosti vlivu různého poměru dvou cest v TERO na kvalitu výstupu?

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Celkové hodnocení

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.