FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Buček, Ph.D.
Student:	Daniel Jantošovič
Název práce:	Implementace TRNG založeného na SRAM na mikrokontroléru
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	6. června 2022

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 v plném rozsahu.

2. Písemná část práce 78 /100 (C)

Písemná část práce je logicky členěná a přehledná. Všechny části jsou rozsahem přiměřené. V kapitole 4.1 student ukazuje zajímavé grafy průměrné hodnoty bitů v paměti v závislosti na čase vypnutí. Bylo by vhodné také uvést teplotu, při které bylo měření prováděno. U grafů směrodatné odchylky bohužel student neuvádí, které přesně veličiny se směrodatná odchylka počítá (a jakým způsobem).
Práci by prospělo důkladněji se zamyslet nad scénářem použití vytvořeného generátoru a také nad postupem testování a vyhodnocením testů. V práci nebyl představen generátor ve formě, kdy by byl použitelný pro nějaký další (třeba i simulovaný) účel přímo v zařízení, ale generované číslo se rovnou pošle po sériové lince do PC. To je užitečné pro následné testování v PC, ale není jasné, jak by náhodné číslo mohla využít aplikace přímo na mikrokontroléru. K tomu by byl vhodný i nějaký detailnější diagram ve kapitole o návrhu (obr. 3.1 je stejný jako obr. 2.10, a je příliš strohý).
Co se týká testování, student použil baterii statistických testů NIST Statistical Test Suite (NIST SP 800-22), což je rozumná volba, a použil ji vhodným způsobem (počet opakování, délka posloupnosti). Co už není tak vhodné, je, že student testoval výstup generátoru až po postprocessingu pomocí SHA256. Takový test nám mnoho neřekne, protože SHA256 "smaže" všechny nedokonalosti. Pokud se vstup do hašovací funkce nezopakuje kompletně identicky, haš bude vždy randomizována a testy nemohou nic najít. Případné zopakování vstupních dat by se dalo otestovat mnohem snadněji. Pro ilustraci, kdybychom místo syrových dat TRNG hašovali čítač, pokud čítač nerestartujeme, výstupy

haší vždy testy projdou. O náhodnosti vstupu nám to nic neřekne (čítač rozhodně náhodný není).
Po formální stránce jsou v práci patrné nedostatky v úpravě, například chybějící mezery mezi slovem a závorkou, odkazy na obrázky (např. "Na 5.1" místo "Na obrázku 5.1") apod.

3. Nepísemná část, přílohy 75 /100 (C)

Přílohou jsou jednak tři varianty firmware pro mikrokontrolér pro různé varianty experimentu a dále skripty pro vyhodnocení na PC (ve formě Jupyter notebooků v Pythonu). Student také přikládá měřená data (i když vstup pro NIST STS přiložen není). V odevzdaném kódu nejsou studentovy zdrojáky podepsány (označeny v komentáři) jeho jménem, což ztěžuje rozlišení, co je jeho práce, a co je převzaté.

4. Hodnocení výsledků, jejich využitelnost 79 /100 (C)

Výsledky studentovy práce mohou být užitečné jako základ pro demonstraci a další experimenty s TRNG na mikrokontroléru ARM.

Celkové hodnocení 79 /100 (C)

Student prokázal schopnost samostatné tvůrčí práce. Výsledkem je zajímavý experiment s náhodným generátorem na mikrokontroléru. Vzhledem k výše uvedeným skutečnostem doporučuji práci k obhajobě a hodnotím známkou dobře.

Otázky k obhajobě

Čeho přesně směrodatná odchylka je vykreslena na grafech v obr. 4.2 a 4.4, a jak byla spočítána?

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.