FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Filip Štěpánek
Student:	Martin Mandík
Název práce:	Analýza TPM komunikace za pomoci FPGA
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	5. 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 -- výstupem je funkční návrh pro FPGA zařízení, které je schopné zachytávat předem specifikovaný provoz na LPC sběrnici týkající se TPM komunikace. Na základě analýzy byla výsledná množina případů užití zaměřena na přenos BitLocker klíčů (VMK). Nad rámec zadání student implementoval i simulátor LPC / TPM transakcí pomocí přípravku Arduino.

2. Písemná část práce

90 / 100 (A)

Závěrečná práce je psaná v anglickém jazyce a obecně je na velmi vysoké úrovni -- text je čtivý, dobře strukturovaný a obsahuje dostatek informací, aby čtenář pochopil, jak student postupoval, z jakých částí se výstup skládá a jakých bylo dosaženo výsledků.

Mám zde pouze menší výtku k obsahové části -- z hlediska technického výstupu mi schází podrobnější popis implementace stavového automatu, konkrétně jestli student řešil realizaci podle typu "Moore" anebo "Mealy". Informaci jsem zjistil až po prostudování příloh. Dále student musel řešit přechod mezi hodinovými doménami pro FPGA a myslím si, že by téma mělo být více rozebráno v textu.

3. Nepísemná část, přílohy

95 / 100 (A)

Výsledné soubory pro HDL Verilog jsem zkontroloval a provedl vlastní syntézu -- návrh je funkční a dostatečně otestovaný simulační sadou i HW simulátorem LPC sběrnice, který si student za tímto účelem vytvořil. Návrhové soubory by mohly být lépe členěny a

obsahovat více komentářů, ovšem chápu, že student začínal s jazykem Verilog bez předchozích zkušenosti, tedy drobné výtky nezahrnuji do hodnocení.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Výsledný studentův návrh jsem vyzkoušel na svém vlastním PC se zapnutým BitLockerem a připojenou FPGA vývojovou deskou Arty A7 do LPC sběrnice . Provoz TPM za zvolených parametrů jsem zachytil a podle studentova postupu bylo možno zjistit hodnotu VMK nutnou pro následné odemknutí pevného disku. Výstup je porovnatelný s podobnými řešeními zabývajícími se analýzou TPM provozu ať už pomocí logického analyzátoru anebo FPGA, která jsou volně k dispozici. Z hlediska nastavených cílů je výsledek funkční, ale nemyslím si, že bude rozšiřitelný o další případy užití z důvodu statického návrhu a HW omezení mimo studentův dosah (propustnost sériové linky). Avšak jako vstupní krok do problematiky TPM interakcí je výstup povedený a zajisté otevřel studentovi cestu k dalšímu zkoumání TPM.

Celkové hodnocení 95 /100 (A)

Výslednou práci hodnotím jako velmi zdařilou jak po stránce písemné tak i technické. Student si v rámci analýzy a realizace nastudoval velké množství informací z oblastí, ve kterých neměl předchozí zkušenosti (konkrétně: problematika TPM, tvorba návrhu pro FPGA) a dokázal je zpracovat a proměnit ve funkční celek. I když student neměl během realizace přístup k funkčnímu TPM 2.0, byl schopen najít cestu, jak dostatečně testovat fyzický výstup vlastním simulátorem a také se věnovat analytické části za pomoci předem dodaného zachyceného TPM provozu. Výsledný návrh jsem úspěšně vyzkoušel na svém zařízení a výsledky jsem předal studentovi k prezentaci při obhajobě.

Otázky k obhajobě

Hlavní bod závěrečné práce se zabývá návrhem stavového automatu, který pasivně analyzuje komunikaci na sběrnici. Z textu není patrné, o jaký druh automatu se jedná -- můžete popsat, jestli jste použil automat typu Moore anebo Mealy, jaké výhody pro návrh z toho vyplynuly, případně jak se jejich implementace liší ve zvoleném HDL Verilog?

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.