FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Dr.-Ing. Martin Novotný
Student:	Vít Mašek
Název práce:	Víceúčelová hardwarová platforma pro kryptografii nad eliptickými křivkami
Obor / specializace:	Počítačové inženýrství
Vytvořeno dne:	1. 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

Předložená bakalářská práce svým rozsahem naplňuje požadavky kladené na diplomové práce a možná je i překračuje. Přesto dokumentuje pouze část patnáctiměsíční práce autora. Zadání práce se pozměňovalo a precizovalo, a proto autor v průběhu práce vytvořil několik větví řešení. V textu ale pro přehlednost dokumentuje pouze tu větev, která odpovídá konečné variantě zadání.

2. Písemná část práce

99 / 100 (A)

Práce je členěná přehledně, text je čitelný a je informačně bohatý. Oceňuji zejména kapitolu State of the Art, která shrnuje nezbytné teoretické základy pro následnou inženýrskou práci. Autor průběžně diskutuje varianty řešení finálního zadání. Vzhledem k rozsahu prací autor pro přehlednost vynechal informace o jednotkách, které vytvořil, ale které nejsou začleněny do výsledného návrhu.

3. Nepísemná část, přílohy

100 / 100 (A)

Textové přílohy obsahují informaci o navržené ISA, rozhraních a adresovém prostoru. Přiložené paměťové médium obsahuje velmi dobře komentované zdrojové kódy a dále kódy pro testbenche a generátory testovacích dat napsané ve Wolfram Mathematica.

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

Předložená práce je součást většího celku - kryptografického procesoru, který by se měl vyrábět jako zákaznický obvod (ASIC). Zadavatelem je firma TropicSquare.
Část výsledků bakalářské práce byla rovněž prezentována na mezinárodní konferenci DDECS 2022.

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Scházeli jsme se na pravidlených týdenních schůzkách.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Bez výhrad.

Celkové hodnocení 100 /100 (A)

Předložená bakalářská práce svým rozsahem naplňuje požadavky kladené na diplomové práce a možná je i překračuje. Přesto dokumentuje pouze část patnáctiměsíční práce autora. Zadání práce se pozměňovalo a precizovalo, a proto autor v průběhu práce vytvořil několik větví řešení. V textu ale pro přehlednost dokumentuje pouze tu větev, která odpovídá konečné variantě zadání.
Předložená práce je součást většího celku - kryptografického procesoru, který by se měl vyrábět jako zákaznický obvod (ASIC). Zadavatelem je firma TropicSquare.
Část výsledků bakalářské práce byla rovněž prezentována na mezinárodní konferenci DDECS 2022.
Vzhledem k rozsahu a kvalitě předložené práce si dovoluji komisi navrhnout, aby zvážila její navržení na cenu děkana.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.