FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Dr.-Ing. Martin Novotný
Student:	Bc. Pavel Chytrý
Název práce:	FPGA akcelerace baby varianty schématu WTFHE
Obor / specializace:	Návrh a programování vestavných systémů
Vytvořeno dne:	25. srpna 2021

Hodnotící kritéria

1. Splnění zadání

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

Zadání hodnotím jako náročné. Diplomová práce se pohybuje v oblasti homomorfního šifrování, což je aktuální výzkumné téma. Konkrétně, prozkoumává možnosti FPGA akcelerace schématu WTFHE. V průběhu řešení práce se několikrát iterovaly parametry zadání tak, jak se průběžně upřesňovaly parametry schématu WTFHE a jak byla získávána zpětná vazba ze zjištěných postsyntézních veličin.

2. Písemná část práce 75 /100 (C)

Práce je členěna správně a přehledně. Nižší hodnocení dávám vzhledem k těžkopádnosti textu.

3. Nepísemná část, přílohy 89 /100 (B)

Kód je členěn přehledně, přivítal bych více komentářů.

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Cílem práce byl průzkum bojem, tedy zjištění, na jaké problémy narazíme při akceleraci schématu WTFHE na FPGA. To práce skutečně splnila, nyní už jsme zkušenější. Ačkoliv zatím nemáme k dispozici akceleraci plnoprávného schématu, ale pouze jeho baby varianty, domnívám se, že i tyto předběžné výsledky jsou publikovatelné.

5. Aktivita studenta

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

Student pravielně konzultoval každý týden.

6. Samostatnost studenta

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

Řadu postupů a řešení navrhnul student sám, některé byly výsledkem konzultace.

Celkové hodnocení 85 /100 (B)

Předložená diplomové práce je poměrně náročná jak co se týče rozsahu prací, tak co se týče novátorské problematiky a poměrně složitého matematického aparátu. Student splnil zadání, tedy vytvořil akcelerátor baby varianty schématu WTFHE. Dosažené výsledky již lze publikovat. Text je však místy těžkopádný, proto navrhuji hodnotit práci známkou B.

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.