FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Posudek oponenta závěrečné práce

| | |
|---|---|
| **Oponent práce:** | Ing. Jakub Klemsa |
| **Student:** | Bc. Pavel Chytrý |
| **Název práce:** | FPGA akcelerace baby varianty schématu WTFHE |
| **Obor / specializace:** | Návrh a programování vestavných systémů |
| **Vytvořeno dne:** | 19. 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 bylo bezvýhradně splněno, konkrétně šlo o:
* seznámení se se šifrou TFHE a její variantou WTFHE,
* návrh parametrizovatelného obvodu "od nuly":
* vhodná dekompozice větších celků do menších bloků,
* složení těchto bloků do funkčního celku,
* výběr vhodných výpočetních prostředků v rámci doporučené platformy ZedBoard,
* zjištění mezí parametrů, pro které je ještě možné obvod sestavit pro danou platformu,
* implementaci demo programu, který vyhodnotí jednoduchou neuronovou síť na zašifrovaných datech.

Slabší stránkou práce se ukázala formulace problému (pro nezasvěceného čtenáře by bylo uvedení do problému poněkud obtížněji stravitelné) a také zhodnocení dosažených výsledků.

Obecně musím konstatovat, že se jednalo o náročné téma, předně s ohledem na kontinuální vývoj v teoretické rovině. Student však nové poznatky velice pružně implementoval do svojí práce, s případným překonáváním vyvstanuvších překážek si pak vedl zjevně bez větších obtíží.

### 2. Písemná část práce

60 / 100 (D)

Práce obsahuje relevantní informace, jen místy zabíhá do velkých detailů, což na druhou stranu akcentuje rozsah řešeného problému.

Po věcné stránce obsahuje práce některé nepřesnosti v teoretické rovině, což ve výsledku nemělo na splnění zadání žádný vliv, vzniká tím tedy jen pár nepřesností (např. "order of polynomial P" -> "degree of polynomial P", "Torus field" -- Torus není algebraické těleso, "negacyclic set T^(N)[X]" -- tato konkrétní struktura není ničím negacyklická, a další).

Struktura práce odpovídá její povaze, hodnotím ji jako vhodnou.

Celková srozumitelnost textu trpí slabším úvodem do problematiky (jak již bylo konstatováno), z čehož například pramení nejasnost, zda se je akcelerována jen operace bootstrapování (jak se píše např. v Abstraktu), nebo je akcelerováno celé vyhodnocení neuronové sítě (jak se píše v kapitole Introduction). Dále mi chybí srozumitelnější úvod do samotného bootstrapování. Trochu matoucí je i prohazované pořadí operandů ve Vector-Matrix násobení, chybějící zmínka o rozílu posledních dvou sloupců v popisku tabulky 6.1 a jednoznačný výčet přenášených dat v sekci 6.2.2.

Po typografické stránce jsou nejvíce do očí bijící přetékající řádky, po jazykové stránce potom špatně volené členy a výjimečně i slovíčka (např. safety vs. security).

Student se odkazuje na relevantní literaturu a správným způsobem ji cituje. Například v první kapitole, jejíž obsah je převážně vytvořen z materiálů k nastudování, se na tyto zdroje přímo odkazuje.

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

Student využil své předchozí zkušenosti z programování platformy Nexys3, bez větších potíží potom přizpůsobil svůj kód nově doporučené platformě ZedBoard. Výkonnější platforma ZedBoard byla v době začátku psaní práce doporučena z důvodu velké očekávané náročnosti, což se ukázalo jako krok správným směrem -- bývaly by byly využity i větší zdroje, než které dokáže ZedBoard nabídnout.

Logické členění bylo kódu zřetelné, rozdělení mezi hardware a software bylo důkladně analyzováno a podle návrhu i provedeno. Velkým plusem implementace je nezávislá testovatelnost jednotlivých komponent.

### 4. Hodnocení výsledků, jejich využitelnost 75 /100 (C)

Cílem práce je "průzkum terénu", není tedy přímo určena k praktickému nasazení. Vskutku, hlavním cílem práce bylo, cituji, "determine the FEASIBILITY of accelerating the WTFHE Scheme on an FPGA". Jako průzkum terénu svůj účel splňuje.

Opět bych vytkl nižší kvalitu provedení slovního hodnocení dosažených výsledků.

## Celkové hodnocení 70 /100 (C)

Své hodnocení opírám o dvě, trochu protichůdné, roviny práce.

V rovině splnění zadání se práce -- i přes mnoho nepředvídatelných překážek -- opravdu povedla:
1) podařilo se rozjet WTFHE bootstrapování na FPGA,
2) ukázaly se všechny limity, což určitě poslouží do budoucna jako dobrý základ pro rozhodování, kterou platformu pro nejrychlejší možné WTFHE bootstrapování zvolit.
Hodnotím 100/100.

V rovině sepsání do textu se projevily:
1) velká časová náročnost samotné implementace,
2) studentova těžkopádnost ve psaní textů spolu s nižší dovedností předávat informace.
Bod 1) je fakticky zahrnut ve výborném hodnocení v rovině splnění zadání a rozhodně nemůže být výmluvou, proto nezávisle hodnotím sepsaný text skórem 50/100.

## Otázky k obhajobě

1) Okomentujte možnost generování bootstrapovacích klíčů ze seedu pomocí proudové šifry.
2) Jak moc by bylo náročné v implementaci nahradit operaci POLY_MULT (negacyklické násobení polynomů) analogickou operací využívající Fourierovu transformaci?

# 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.