Posudek oponenta bakalářské práce

Student: Linner Marek
Téma: Hardwarová akcelerace šifrovacích algoritmů s technologií Xilinx Zynq (id 24118)
Oponent: Fukač Tomáš, Ing., UPSY FIT VUT

1. Náročnost zadání

průměrně obtížné zadání

Zadání práce si vyžadovalo prostudování šifrovací algoritmy DES a AES, navrhnout a implementovat jejich obvodovou realizaci s ohledem především na propustnost a srovnat ho se softwarovým řešením. Zadání celkově hodnotím jako standardně složité.

2. Splnění požadavků zadání

student se odůvodněně odchýlil od zadání s vážnými výhradami

Původní znění zadání práce si vyžadovalo analýzu rozdělení implementace mezi hardwarové a softwarové zdroje. Tento bod zadání byl nejspíše po konzultaci s vedoucím práce změněn na čistě obvodovou realizaci (vyplývá z hodnocení vedoucího práce), v práci však není jediné odůvodnění tohoto odklonu od původního zadání. Práce navíc postrádá popis přípravku ZynqBerry, což si vyžaduje 2. bod zadání.

3. Rozsah technické zprávy

je v obvyklém rozmezí

Text práce je odhadem v obvyklém rozmezí, přesný počet normostran nebylo možné odvodit, protože autor práce do odevzdaných souborů nepřiložit zdrojové soubory textu práce.

4. Prezentační úroveň předložené práce

65 b. (D)

Jednotlivé kapitoly na sebe logicky navazují a jejich rozsah většinou odpovídá popisové problematice. Úvod je však nepřiměřeně dlouhý (přibližně 2,5 stránky), oproti tomu kapitola popisující testování má pouze jeden krátký odstavec, což považuji za nedostačující. Text je často doplněn názornými obrázky a tabulkami, které pomáhají čtenáři pochopit popisovanou problematiku, často jsou však nepřiměřeně velké či obsahují zbytečné informace (např. tabulky popisující zrychlení obvodové realizace obsahují informace o *popularitě* atd). U rychlostí softwarových implementací dále není uvedeno, na jakém zařízení byla měřena. Příklady občas obsahují nekonzistenci (resp. chybu) oproti textu (např. na stránce 8 je chyba v posledním příkladu výplně).

5. Formální úprava technické zprávy

70 b. (C)

Po jazykové stránce text práce obsahuje menší množství překlepů, nevhodně použitých slov a slovních obratů, doslovné české překlady některých anglických názvů, pro zkoumanou oblast odlišná pojmenování oproti běžně používaným. Po typografické stránce text obsahuje často jednoslabičné předložky na konci řádků, sirotky (např. stránka 19).

6. Práce s literaturou

65 b. (D)

V práci jsou použity prameny, které jsou voleny vhodně s ohledem na téma práce. Citace pramenů je v textu však uvedena jen zřídka a je proto obtížné odlišit převzaté prvky a špatně se určuje pramen (např. úvod obsahující historická fakta a faktické informace obsahuje jen jednu citaci). U rozsáhlých knižních titulů by bylo vhodné uvést i strany, ze kterých bylo čerpáno.

7. Realizační výstup

45 b. (F)

Realizační výstup je funkční, což bylo ověřeno vytvořeným testem. Výsledné šifrovací obvody však běží na relativně nízkých frekvencích. Ta je dostačující pro přípraven ZynqBerry, pro reálné nasazení by nemusela být dostačující. Dešifrovací obvody nebyly zřetězeny vůbec. Odůvodnění, že zřetězení by bylo náročné, beru jako irelevantní, do obvodu stačilo pouze přidat registry pro uchování subklíčů. Obvody bez zřetězení běží na velmi malé frekvenci a pro použití v praxi jsou proto nepoužitelné. Například propustnost dešifrovací jednotka algoritmu AES je jen přibližně dvojnásobná oproti softwarovému řešení, ale vyžaduje si většinu hardwarových zdrojů FPGA čipu Zynq. Práce také nespecifikuje, na jakém zařízení byla odvozena propustnost softwarových řešení. Pokud proběhlo na nevýkonném embeded procesoru, mírné navýšení výkonu by bylo na úkor použití výrazně dražšího FPGA čipu.
Výsledné komponenty navíc neobsahují žádné validační signály, není proto jasné, kdy je výstup platný, v práci

není ani odvozeno zpoždění obvodu.
Dle autora práce byl pro eliminaci vzniku chyby při implementaci některých základních VHDL komponent vytvořen složitý generátor, jehož zdrojové kódy nejsou nijak komentovány. To mohlo zapříčinit vznik spoustu jiných chyb, navíc kód generátoru je díky absenci komentář jen špatně uchopitelný a znovupoužitelný.

8. Využitelnost výsledků

Výsledky práce jsou spíše implementačního charakteru. Komponenty pro šifrování by byly použitelné v praxi, kdyby obsahovaly na výstupu signál značící, že výstupní data jsou validní. Komponenty pro dešifrování nejsou zřetězeny, jejich pracovní frekvence a propustnost z toho vyplývající je proto velmi nízká a implementované obvody jsou v praxi nepoužitelné.

9. Otázky k obhajobě

- Na jakém zařízení bylo provedeno měření propustnosti softwarové implementace šifrovacích algoritmů?
- V textu práce je uvedeno, že se spouštěním softwarové implementace je spjata jistá režie na vytvoření vnitřních struktur adt. Neuvažoval jste měření pouze části algoritmu provádějící čistě šifrování, čímž by bylo eliminováno zkreslení způsobené uvedenou režií?

10. Souhrnné hodnocení **50 b. dostatečně (E)**

Vzhledem k značným výhradám k technické zprávě, a především k realizačnímu výstupu, uděluji celkové hodnocení **E - dostatečně**.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 3. června 2021

Fukač Tomáš, Ing.
oponent