Posudek oponenta bakalářské práce

Student: Fruněk Lukáš
Téma: Implementace šifrovacích algoritmů v jazyce VHDL (id 23954)
Oponent: Fukač Tomáš, Ing., UPSY FIT VUT

1. Náročnost zadání

obtížnější zadání

Zadání práce si vyžadovalo důkladné prostudování šifrovací algoritmy DES a AES, navrhnout a implementovat jejich optimalizaci s ohledem především na propustnost výsledného obvodu. Pro výsledné obvody bylo navíc požadováno vytvoření funkční verifikace pro ověření funkčnosti implementovaných obvodů, díky čemu považuji zadání za mírně obtížnější.

2. Splnění požadavků zadání

zadání splněno

Všechny body zadání byly splněny.

3. Rozsah technické zprávy

je v obvyklém rozmezí

Rozsah předložené technické zprávy je v obvyklém rozmezí a text je často doplněn relevantními obrázky.

4. Prezentační úroveň předložené práce

75 b. (C)

Jednotlivé kapitoly na sebe logicky navazují, jejich rozsah odpovídá popisované problematice. Text je informačně bohatý a často doplněn názornými obrázky. Text popisující obrázek však občas používá označení, která nejsou v obrátku použita (např. obr. 2.12 neobsahuje registr *reg*), v závěru strany 13 dokonce odkaz na obrázek chybí (nejspíše překlep v referenci). V textu jsou navíc často používány zkratky, které jsou vysvětleny až o několik stránek dále, nebo nejsou vysvětleny vůbec. Pro čtenáře proto může být text hůře pochopitelný.
Kapitoly popisujících šifrovací algoritmy postrádají teoretický základ. Text popisuje pouze, jak algoritmy fungují, čtenáři však nevysvětluje, na jakém teoretickém principu pracují, proč by měl daný algoritmus fungovat, proč jsou použity uvedené konstanty atd. V kapitole návrhu není uvedena žádná analýza nebo diskuse o kritické cestě obvodu, která je však důležitá pro volbu umístění registrů zřetězené pipeline.
V úvodu kapitoly zabývající se návrhem obvodů jsou uvedeny výsledné parametry finálních obvodů, které patří spíše do výsledků práce (spotřeba zdrojů, maximální frekvence, propustnost). V textu se také objevuje zmínka o přílohách, text práce však žádné neobsahuje.

5. Formální úprava technické zprávy

65 b. (D)

Po jazykové stránce text práce obsahuje větší množství překlepů, nevhodně použitých slov a slovních obratů, nespisovných slov (např. slovo *musejí*), výplňkových slov (především *tedy*) a nekonzistenci pojmů. Z hlediska typografie občas přetéká text a obrázky přes okraj, matematické vzorce obsahují místo znaku násobení hvězdičku, text obsahuje občas jednoslabičnou předložku na konci řádku, slova názvu práce je na úvodní stránce rozděleno.

6. Práce s literaturou

60 b. (D)

V práci jsou použity prameny, které jsou voleny vhodně s ohledem na téma práce. Citace pramenů je v textu uvedena jen zřídka a je proto obtížné odlišit, zda se jedná o převzaté prvky a z jakých pramenů případně pochází (např. úvod neobsahuje jedinou citaci). U knižních titulů by bylo vhodné uvést i strany, ze kterých bylo čerpáno.

7. Realizační výstup

95 b. (A)

Realizační výstup je plně funkční, což bylo ověřeno i vytvořenou funkční verifikací. Implementované komponenty používají standardních rozhraní a dosahují velmi vysoké pracovní frekvence a propustnosti. Zdrojové kódy jsou dostatečně komentovány a popsány v přiloženém souboru README.

8. Využitelnost výsledků

Výsledky práce jsou spíše implementačního charakteru. Komponenty byly již navrhovány tak, aby byly snadno využitelné v praxi použitím standardních rozhraní. Výsledná implementace je ověřena funkční verifikací a dosahuje velmi vysokých propustností. V závěru práce je navíc uvedena úvaha pro navýšení propustnosti až na stovky Gb/s.

9. Otázky k obhajobě

- U režimu ECB uvádíte, že není odolný vůči útoku s výběrem otevřeného textu (chosen-plaintext attack). V čem tento útok spočívá a k čemu ho může útočník zneužít?
- Proč byl pro srovnání propustnosti výsledného řešení se softwarovou implementací vybrán právě ARM Cortex-M4 běžící na velmi nízké frekvenci? Proč nebyla zvolena výkonnější varianta ARM procesoru?

10. Souhrnné hodnocení

75 b. dobře (C)

Realizační výstupy práce jsou velmi kvalitní, ověřené funkční verifikací a snadno použitelné v dalších obvodech. Text technické zprávy však obsahuje řadu nedostatků. Vzhledem k výhradám k technické zprávě uděluji celkové hodnocení **C - dobře**.

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