

Hodnocení vedoucího bakalářské práce

Student: Fruněk Lukáš
Téma: Implementace šifrovacích algoritmů v jazyce VHDL (id 23954)
Vedoucí: Kořenek Jan, doc. Ing., Ph.D., UPSY FIT VUT

1. Informace k zadání

Cílem práce bylo implementovat v jazyku VHDL šifrovací algoritmy AES a DES s cílem optimalizovat obvodovou realizaci na maximální propustnost a ověřit funkci výsledného řešení pomocí funkční verifikace. Díky nutnosti optimalizovat návrh a současně vytvořit funkční verifikace považuji zadání za mírně obtížnější. Student vytvořil funkční implementaci, která dosahuje vysoké propustnosti.

2. Práce s literaturou

Student čerpal jak z literatury doporučené, tak z literatury získané vlastní aktivitou.

3. Aktivita během řešení, konzultace, komunikace

V zimním semestru byla práce konzultována jen málo, v letním semestru již probíhaly pravidelné konzultace, a to v online formě. Student postupoval systematicky, na konzultace byl připraven a řešené problematice rozuměl.

4. Aktivita při dokončování

Práce byla dokončena v termínu a obsah i výsledky byly před odevzdáním v předstihu konzultovány.

5. Publikační činnost, ocenění

Výsledky práce jsou spíše implementačního charakteru. Z práce nevznikla žádná publikace a ani se žádná publikace do budoucna neplánuje.

6. Souhrnné hodnocení

velmi dobře (B)

Student se seznámil s šifrovacími algoritmy DES a AES a pro oba algoritmy navrhl obvodovou realizaci. Obvody implementoval v jazyku VHDL a postupně optimalizoval z pohledu propustnosti a spotřeby hardwarových zdrojů. Vytvořenou implementaci následně důkladně ověřil prostřednictvím funkční verifikace. Vzhledem k mírně složitějšímu zadání, kvalitním parametrům obvodové realizace a praktické použitelnosti výsledného řešení navrhuji hodnocení stupněm B (velmi dobře).

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

V Brně dne: 26. května 2021

Kořenek Jan, doc. Ing., Ph.D.
vedoucí práce