УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 04.07.2018. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Илије Ђурића, дипл. инж. Електротехнике и рачунарства, под насловом „Хардверска имплементација AES алгоритма у бројачком моду“. Након прегледа материјала комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Илија Ђурић је рођен 15.05.1989. године у у Аустралији. Завршио је основну школу "Бранко Радичевић" у Београду са одличним успехом. Уписао је Математичку гимназију у Београду и коју је завршио са врло добрим успехом. Током школовања ишао је на курсеве енглеског језика у Оксфорду и Лондону. Електротехнички факултет уписао је 2008. године. Дипломирао је на одсеку за Телекомуникације и информационе технологије 2016. године са просечном оценом 7,20. Дипломски рад одбранио је у септембру 2016. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за системско инжењерство и радио комуникације уписао је у октобру 2016. године. Током мастер студија радио је двомесечну праксу у Микроелектроници. Положио је све испите са просечном оценом 8,40.

2. Опис мастер рада

Мастер рад обухвата 30 страна, са укупно 23 слике, 1 табелом и 8 референци. Рад садржи увод, 3 поглавља, закључак и списак коришћене литературе.

Предмет рада представља хардверску реализацију AES алгоритма у бројачком моду. У тези је коришћен VHDL програмски језик и ISE развојно окружење.

У уводном поглављу је објашњен значај AES алгоритма за шифровање симетричним кључем, наведен је циљ тезе и дат је преглед остатка рада по поглављима.

У другом поглављу је детаљно објашњен AES алгоритам (историјат, структура, намене), а потом је објашњен бројачки мод који се имплементира у раду.

У трећем поглављу је дат кратак опис коришћених алата и програмског језика. Описан је укратко VHDL програмски језик и ISE развојно окружење.

У четвртом поглављу је детаљно приказана реализација AES алгоритма у бројачком моду. Описан је пакет који садржи функције које се користе у рундама AES алгоритма. Потом је описан главни ентитет који имплементира AES алгоритам у бројачком моду. У раду је коришћена најплајн техника за постизање високог протока шифровања и дешифровања. Потом је описана реализација тестирања којом је проверена исправност реализације - описан је поступак и начин симулације реализованог дизајна. На крају је дат преглед перформанси реализоване имплементације.

У петом поглављу је резимиран рад на тези и потом је дат списак коришћене литературе.

3. Анализа рада са кључним резултатима

Мастер рад Илије Ђурића, дипл. инж. Електротехнике и рачунарства, реализује AES стандард за шифровање симетричним кључем у бројачком моду при чему је коришћена пајплајн техника за постизање високе брзине шифровања, односно дешифровања. Основни доприноси рада су следећи:

1) Реализован је хардверски модул који врши шифровање/дешифровање AES алгоритма у бројачком моду;
2) Дизајн је портабилан и може се користити и на чиповима других произвођача;
3) Остварена је подршка за високе протоке шифровања/дешифровања;

4. Закључак и предлог

Кандидат Илија Ђурић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно реализовао хардверску имплементацију AES алгоритма у бројачком моду. Кандидат је показао довољну самосталност и способност да реши проблеме са којима се сусрео током израде тезе. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Илије Ђурића, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 03.09.2018. године

Чланови комисије:

Др Зоран Чича, ванр. професор

Др Дејан Драјић, ванр. професор