КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 06.06.2023. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Дарка Ардалића, дипл. инж. Електротехнике и рачунарства, под насловом „Хардверска имплементација Kalyna алгоритма енкрипције симетричним кључем“. Након прегледа материјала комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Дарко Ардалић је рођен 11.04.1997. године у Београду. Завршио је Основну школу „Павле Савић” у Београду као вуковац. Уписао је Шесту београдску гимназију у Београду, коју је завршио као вуковац. Електротехнички факултет уписао је 2016. године. Дипломирао је на одсеку за Телекомуникације и информационе технологије 2021. године са просечном оценом 7,87. Дипломски рад одбранио је у септембру 2021. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на модулу Информационо-комуникационе технологије уписао је у октобру 2021. године. Положио је све испите са просечном оценом 10,00.

2. Извештај о студијском истраживачком раду

Кандидат Дарко Ардалић је у склопу припреме за мастер рад проучио литературу из области шифровања симетричним кључем. Потом је проучио спецификацију Kalyna алгоритма за шифровање симетричним кључем. На крају је осмислио дизајн имплементације наведеног алгоритма. Након обављеног студијског истраживачког рада, Дарко је приступио изради саме тезе.

3. Опис мастер рада

Мастер рад обухвата 39 страна, с укупно 40 слика, 20 табела и 10 референци. Рад садржи увод, 6 поглавља, закључак (укупно 8 поглавља), списак коришћене литературе и списак скраћеница.

Предмет рада је хардверска имплементација Kalyna алгоритма за шифровање симетричним кључем. Циљ рада је креирање пајплајн имплементације алгоритма ради постизања максималног протока шифровања података. Коришћен је VHDL језик за опис хардвера. Коришћено развојно окружење је ISE компаније Xilinx.

У уводном поглављу је изложен значај шифровања података, предмет тезе и на крају је дат детаљан преглед остатка тезе по поглављима.

Друго поглавље даје кратак теоријски осврт на област шифровања. Изложена је улога шифровања и класификација алгоритама. На крају су дати аспекти које треба узети у обзир приликом избора алгоритма за жељену примену.

Треће поглавље садржи опис Kalyna алгоритма за шифровање симетричним кључем. Изложени су сви саставни делови алгоритма с одговарајућим објашњењима и математичком позадином сваке од функција алгоритма.

Четврто поглавље даје преглед коришћених алата и развојног окружења с кратким описима.

Пето поглавље даје опис хардверске имплементације. Описана је архитектура дизајна као и саставни делови, односно компоненте реализованог дизајна. Описан је коришћени пајплајн принцип за постизање максималног протока шифровања.

У шестом поглављу је описана симулација дизајна која је коришћена за верификацију исправности рада реализованог дизајна. Симулирани, односно верификовани су како појединачни делови дизајна, тако и комплетан дизајн. У седмом поглављу су дати резултати верификације где су за сваку компоненту, као и комплетан дизајн дати тест вектори и очекивани резултат, а потом су приказани резултати симулације који потврђују да су добијени очекивани резултати чиме је потврђено да је дизајн успешно реализован.

Осмо поглавље резимира резултате тезе, а потом су дати списак коришћених референци и списак скраћеница.

4. Анализа рада са кључним резултатима

Мастер рад Дарка Ардалића, дипл. инж. Електротехнике и рачунарства, се бави пајплајн реализацијом Kalyna алгоритма за шифровање симетричним кључем. Кључни доприноси рада кандидата на тези су следећи:

1) дато детаљно објашњење свих делова Kalyna алгоритма;
2) реализована пајплајн имплементација Kalyna алгоритма;
3) реализована имплементација је портабилна и може се користити на програмабилним чиповима различитих произвођача.

5. Закључак и предлог

Кандидат Дарко Ардалић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно реализовао Kalyna алгоритам за шифровање симетричним кључем. Дарко је показао велику самосталност приликом рада на тези и брзо је решавао проблеме на које је наилазио приликом имплементације. Предложено решење се може користити у мрежним уређајима за потребе шифровања података. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Дарка Ардалића, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 08.09.2023. године

Чланови комисије:

др Зоран Чича, ред. професор

др Дејан Драјић, ред. професор