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 22.05.2018. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Андријане Продановић, дипл. инж. Електротехнике и рачунарства, под насловом „Минимална хардверска имплементација Camellia алгоритма за шифровање". Након прегледа материјала комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Андријана Продановић је рођена 13.02.1993. године у Фочи. Завршила је основну школу "Веселин Маслеша" у Фочи као вуковац. Уписала је Општу гимназију у Фочи и коју је завршила као вуковац и ђак генерације. Електротехнички факултет уписала је 2012. године. Дипломирала је као студент на одсеку за Телекомуникације и информационе технологије 2016. године са просечном оценом 8,04. Дипломски рад одбранила 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 уписала је у октобру 2016. године. Положила је све испите са просечном оценом 8,60.

2. Опис мастер рада

Мастер рад обухвата 43 стране, са укупно 12 слика, 5 табела и 6 референци. Рад садржи увод, 6 поглавља, закључак (укупно 8 поглавља), списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Предмет рада представља минималну хардверску имплементацију Camellia алгоритма за симетрично шифровање. Приликом израде тезе, за израду имплементације, коришћен је VHDL програмски језик и ISE развојно окружење.

У уводном поглављу је наведен значај безбедности у модерним телекомуникацијама, потом је наведен циљ тезе и на крају је изложена структура остатка тезе по поглављима.

У другом поглављу су дати и укратко објашњени основни појмови из области криптографије, наведена је класификација алгоритама за шифровање и наведени су најпознатији алгоритми за шифровање.

У трећем поглављу су објашњене градивне функције које сачињавају Camellia алгоритам за шифровање.

У четвртом поглављу је описана структура процеса шифровања, а у петом поглављу је описана структура процеса дешифровања.

У шестом поглављу је описана хардверска имплементација и блока за шифровање и блока за дешифровање, при чему су на почетку поглавља објашњене реализације градивних функција. Објашњења су пропраћена и приложеним програмским кодовима. Реализована имплементација је организована тако да користи што мање ресурса на чипу. Приликом имплементације, коришћен је VHDL програмски језик и ISE развојно окружење.

У седмом поглављу је дат опис верификације дизајна која је потврдила функционалну исправност реализације. Потом је дат преглед перформанси у виду заузећа ресурса и за блок за шифровање и за блок за дешифровање.

У осмом поглављу су резимирани резултати рада на тези и потом је дат списак коришћене литературе, списак скраћеница, списак слика и списак табела.

3. Анализа рада са кључним резултатима

Мастер рад Андријане Продановић, дипл. инж. Електротехнике и рачунарства, је реализовао минималну хардверску имплементацију Camellia алгоритма за шифровање. Основни доприноси рада су следећи:

1) релизована минимална хардверска имплементација Camellia алгоритма за шифровање;
2) реализована имплементација је портабилна и може се користити на чиповима различитих произвођача;

4. Закључак и предлог

Кандидат Андријана Продановић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно реализовала минималну хардверску имплементацију Camellia алгоритма за шифровање. Андријана је успешно решила све проблеме на које је наишла током израде тезе, показала је способност самосталног рада, као и квалитетног презентовања резултата свог рада на тези. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Андријане Продановић, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 14.09.2018. године

Чланови комисије:

др Зоран Чича, ванр. професор

др Дејан Драјић, ванр. професор