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 29.08.2017. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Филипа Никића под насловом „Хардверска имплементација ARIA алгоритма за шифровање симетричним кључем". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Филип Никић је рођен 01.05.1993. године у Београду. Завршио је основну школу "Радојка Лакић" у Београду са одличним успехом. Уписао је Прву београдску гимназију у Београду и коју је завршио са одличним успехом. Електротехнички факултет уписао је 2012. године. Дипломирао је на модулу за Телекомуникације и информационе технологије, одсек Системско инжењерство, 2016. године са просечном оценом 8,65. Дипломски рад „Веб туторијал из оптичких приступних мрежа" одбранио је у јулу 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.

2. Опис мастер рада

Мастер рад обухвата 85 страна, са укупно 14 слика, 3 табеле и 13 референци. У прилогу је дат комплетан програмски код имплементације. Рад садржи увод, 4 поглавља, закључак (укупно шест поглавља) и литературу. Предмет рада је хардверска имплементација модула за шифровање и дешифровање ARIA алгоритмом, при чему је имплементација реализована тако да постигне максималну брзину шифровања/дешифровања. Коришћено је ISE развојно окружење, а имплементација је реализована употребом VHDL програмског језика.

У уводном поглављу је изложен циљ и предмет мастер тезе, а потом је дат преглед остатка тезе по поглављима.

У другом поглављу су дате основне дефиниције, историјат и класификација криптографије.

У трећем поглављу је дат детаљан опис ARIA алгоритма за шифровање.

Четврто поглавље садржи детаљан опис хардверске имплементације ARIA алгоритма. Детаљно су описани сви делови имплементације, а програмски код је дат у прилогу да основни текст тезе не би био непрегледан. Имплементација користи пајплајн технику за постизање максималне брзине шифровања/дешифровања.

Пето поглавље садржи опис верификације исправности рада реализованог модула, а такође је дата табела са перформансама реализоване имплементације.

На крају тезе је изложен закључак који сумира резултате рада. На крају рада дата је литература, са 13 референци, која је коришћена приликом израде мастер рада, као и прилог са комплетним програмским кодом реализоване имплементације.

3. Анализа рада са кључним резултатима

Мастер рад Филипа Никића, дипл. инж. Електротехнике и рачунарства, бави се хардверском реализацијом модула који врши шифровање и дешифровање ARIA алгоритмом.

Основни доприноси рада су: 1) реализован модул за шифровање и дешифровање ARIA алгоритмом; 2) реализовано решење користи пајплајн технику за постизање максималне брзине шифровања/дешифровања; 3) решење је портабилно и може се користити и на чиповима других произвођача (имплементација из ове тезе је реализована на FPGA чипу компаније Xilinx).

4. Закључак и предлог

Кандидат Филип Никић је у свом мастер раду успешно реализовао модул за за шифровање и дешифровање ARIA алгоритмом, при чему реализација омогућава максималне брзине шифровања/дешифровања. Филип је показао упорност у изради тезе и успео је да реши проблеме на које је наишао.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Филипа Никића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 31.08.2017. године

Чланови комисије:

Др Зоран Чича, доцент

Др Дејан Драјић, доцент