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 16.05.2017. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Милића Џакуле под насловом „Имплементација бројачког и ланчаног мода Camellia алгоритма за шифровање". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Милић Џакула је рођен 12.03.1990. године у Карловцу. Завршио је основну школу "Доситеј Обрадовић" у Вражогрнцу као вуковац. Уписао је Техничку школу у Зајечару и коју је завршио као ђак генерације. Електротехнички факултет уписао је 2009. године. Дипломирао је на одсеку за Телекомуникације и информационе технологије 2015. године са просечном оценом 7,74. Дипломски рад одбранио је у октобру 2015. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу Системско инжењерство и радио комуникације уписао је у октобру 2015. године. Положио је све испите са просечном оценом 8.

2. Опис мастер рада

Мастер рад обухвата 38 страна, са укупно 11 слика, 6 табела и 9 референци. Рад садржи увод, 6 поглавља, закључак (укупно осам поглавља) и литературу. Предмет рада је хардверска имплементација бројачког и ланчаног мода Camellia алгоритма за шифровање. 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 дефинисани основни појмови који се користе у криптографији. Укратко је објашњена улога и циљ криптографије, и изложени су основни принципи рада алгоритама за шифровање симетричним кључем, као и алгоритама за шифровање асиметричним кључем.

У трећем поглављу је дат опис Camellia алгоритма за шифровање. Објашњен је начин рада овог алгоритма, и описани су сви саставни делови алгоритма.

У четвртом поглављу су наведени начини допуне (у виду модова) основног рада блоковског алгоритма за шифровање симетричним кључем (у који спада и Camellia алгоритам). Потом су детаљно објашњени ланчани и бројачки мод који су имплементирани у оквиру тезе.

У петом поглављу је детаљно објашњена имплементација бројачког и ланчаног мода. Коришћени су резултати једног ранијег мастер рада (реализација Camellia алгоритма у основном моду) и на те резултате су примењени ланчани, односно бројачки мод који су детаљно описани у поглављу. Релевантни делови кода су приложени у оквиру овог поглавља.

Шесто поглавље садржи опис верификације исправности рада реализованог дизајна, и за бројачки и за ланчани мод, при чему су дата објашњења која омогућавају читаоцу да лако испрати тестове који су рађени у циљу верификације.

Седмо поглавље приказује анализу перформанси реализованих модула у виду одговарајућих табела које приказују потрошњу ресурса чипа.

На крају тезе је изложен закључак који сумира резултате рада. На крају рада дата је литература, са 9 референци, која је коришћена приликом израде мастер рада.

3. Анализа рада са кључним резултатима

Мастер рад Милића Џакуле, дипл. инж. Електротехнике и рачунарства, бави се хардверском реализацијом бројачког и ланчаног мода Camellia алгоритма за шифровање. Основни доприноси рада су: 1) реализован модул за бројачки мод Camellia алгоритма за шифровање; 2) реализован модул за ланчани мод Camellia алгоритма за шифровање; 3) оба модула су портабилна и могу се користити и на чиповима других произвођача (имплементација из ове тезе је реализована на FPGA чипу компаније Xilinx).

4. Закључак и предлог

Кандидат Милић Џакула је у свом мастер раду успешно реализовао модуле бројачког и ланчаног мода Camellia алгоритма за шифровање. Милић је показао познавање области криптографије, као и програмирање у VHDL програмском језику. Успешно је решио све проблеме на које је наилазио током израде тезе.

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

Београд, 11.09.2017. године

Чланови комисије:

Др Зоран Чича, доцент

Др Дејан Драјић, доцент