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 08.06.2021. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Николе Никетића, дипл. инж. Електротехнике и рачунарства, под насловом „Имплементација Kuznyechik алгоритма за шифровање симетричним кључем“. Након прегледа материјала комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Никола Никетић је рођен 04.02.1995. године у Чачку. Завршио је основну школу "Вук Караџић" у Чачку као вуковац. Уписао је природни смер Гимназије у Чачку и коју је завршио са одличним успехом. Електротехнички факултет уписао је 2014. године. Дипломирао је на одсеку за Телекомуникације 2019. године са просечном оценом 8,11. Дипломски рад одбранио је у септембру 2019. 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 2019. године. Положио је све испите са просечном оценом 9,40.

2. Опис мастер рада

Мастер рад обухвата 36 страна, са укупно 8 слика, 1 табелом и 7 референци. Рад садржи увод, 4 поглавља, закључак (укупно 6 поглавља), списак коришћене литературе, списак скраћеница, списак табела и прилог.

Предмет рада представља хардверску имплементацију Kuznyechik алгоритма за шифровање симетричним кључем. Реализована је најплајн имплементација у циљу постизања максималног протока шифрованих података. У раду је коришћен VHDL језик за хардверску имплементацију, као и развојно окружење ISE компаније Xilinx.

Прво поглавље чини увод у коме је прво описан значај безбедности комуникације, потом је наведен предмет рада, и на крају је дат преглед организације тезе по поглављима.

Друго поглавље даје кратак преглед основа криптографије са становишта заштите података, при чему је додатна пажња посвећена Feistel структури која се користи у многим алгоритмима шифровања симетричним кључем укључујући и Kuznyechik алгоритам.

Треће поглавље даје детаљан опис Kuznyechik алгоритма шифровања. Описане су математички све операције и трансформације које се користе у алгоритму.

Четврто поглавље даје детаљан опис реализоване имплементације уз приложен програмски код имплементације. Описани су сви ентитети који се користе у имплементацији почев од хијерархијски највишег ентитета који обавља функцију шифровања, до хијерархијски најнижих ентитета који обављају функције супституције и линеарне трансформације, респективно.

У петом поглављу је описана верификација реализованог дизајна. Коришћене су тест вредности из RFC 7801 документа. Дата је верификација целокупног процеса шифровања, као и верификација линеарне трансформације као најкомпликованије операције у Kuznyechik алгоритму. Такође, процењене су перформансе у погледу постигнутог протока шифровања, као и потребних хардверских ресурса.

Шесто поглавље представља закључак у коме је резимирано шта је урађено у оквиру тезе, као и смернице за будућа унапређења. Потом су дати списак референци, списак скраћеница, списак слика, списак табела и прилог у ком је дат комплетан програмски код за ентитет који врши функцију супституције.

3. Анализа рада са кључним резултатима

Мастер рад Николе Никетића, дипл. инж. Електротехнике и рачунарства, се бави хардверском имплементацијом Kuznyechik алгоритма за шифровање симетричним кључем. Основни доприноси рада су следећи:

1) реализована је пајплајн имплементација Kuznyechik алгоритма за шифровање;
2) реализовани дизајн је портабилан;
3) подржани су протоци реда величине неколико Gb/s.

4. Закључак и предлог

Кандидат Никола Никетић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно реализовао хардверску имплементацију Kuznyechik алгоритма. Никола је показао способност да разуме спецификације алгоритма и потом да те спецификације преточи у хардверски дизајн. Кандидат је показао адекватно познавање VHDL програмског језика и рада у ISE развојном окружењу, као и способност решавања проблема на које је наилазио приликом развоја имплементације. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Николе Никетића, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 16.09.2022. године

Чланови комисије:

др Зоран Чича, ванр. професор

др Дејан Драјић, ванр. професор