

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 24.06.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Александар Прерадовић под насловом „Хардверска имплементација ZUC алгоритма за шифровање засновано на току података“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Александар Прерадовић је рођен 16.06.2000. године у Пљевљима, Црној Гори. Завршио је Основну школу „Ристан Павловић“ у Пљевљима, као носилац дипломе „Луча“. Уписао је Гимназију „Танасије Пејатовић“ у Пљевљима, општи смер, коју је такође завршио као носилац дипломе „Луча“.

Уписује Електротехнички факултет у Београду 2019. године, где се након прве године опредељује за модул Телекомуникације и информационе технологије, а на трећој години бира смер Системско инжењерство. У септембру 2023. године завршио је основне академске студије са просечном оценом 8,02.

Исте године уписује мастер академске студије на Електротехничком факултету, на модулу Информационо комуникационе технологије где је положио све предвиђене испите са просечном оценом 9,22.

2. Извештај о студијском истраживачком раду

Кандидат Александар Прерадовић је прво проучио област криптографије са посебним освртом на алгоритме шифровања симетричним кључем. Проучио је познате алгоритме попут DES, AES, SNOW3G, ZUC. Нарочиту пажњу је посветио ZUC алгоритму који је предмет рада тезе. Упознао се и са развојним окружењем Intel Quartus Prime компаније Altera које се користило у практичном делу тезе. Након урађеног студијског истраживачког рада, Александар је кренуо са израдом своје мастер тезе.

3. Опис мастер рада

Мастер рад обухвата 68 страна, са укупно 9 слика, 8 табела и 7 референци. Рад садржи увод, 4 поглавља, закључак (укупно 6 поглавља), списак коришћене литературе, списак скраћеница, списак слика, списак табела и два прилога.

У уводном поглављу је прво истакнут значај криптографске заштите података. Представљен је предмет и циљ тезе. На крају је изложен преглед садржаја остатка рада по поглављима.

Друго поглавље се бави појмом енкрипције и алгоритмима енкрипције. Изложени су типови алгоритама, а на крају је дат осврт на изазове модерне енкрипције.

Треће поглавље је посвећено опису ZUC алгоритама. Детаљно су описани сви делови ZUC алгоритма и принцип његовог рада.

Четврто поглавље садржи опис хардверске имплементације ZUC алгоритма. За имплементацију је коришћен VHDL програмски језик. Објашњени су сви реализовани модули појединачно, као и њихове међусобне релације.

Пето поглавље представља опис верификације исправности реализоване имплементације. Такође је дат и преглед хардверских ресурса које троши имплементација, као и прорачун подржаног протока шифровања података.

Шесто поглавље резимира резултате мастер тезе и даје смернице за будућа унапређења реализоване имплементације. Потом су дати списак референци, списак скраћеница, списак слика, списак табела, и два прилога који садрже кодове имплементације и тест окружења.

4. Анализа са кључним резултатима

Мастер рад Александра Прерадовића, дипл. инж. Електротехнике и рачунарства, реализује хардверску имплементацију ZUC алгоритма за стрим шифровање. Кључни доприноси рада кандидата на тези су следећи:

- 1) реализована имплементација ZUC алгоритма за стрим шифровање;

- 2) развијено тест окружење за верификацију имплементације;
- 3) реализована имплементација је портабилна и може се користити на програмабилним чиповима различитих произвођача.

5. Закључак и предлог

Кандидат Александар Прерадовић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду реализовао хардверску имплементацију ZUC алгоритма за стрим шифровање. Реализована имплементација се може користити у комуникационим уређајима за шифровање комуникације. Кандидат је показао добро познавање алгоритама енкрипције и генерално област криптографије. Такође је показао способност да самостално и ефикасно уради хардверску имплементацију једног алгоритма енкрипције. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Александра Прерадовића, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 26.09.2025. године

Чланови комисије:

др Зоран Чича Редовни професор
сагласан, 26.09.2025.

др Дејан Драјић Редовни професор
сагласан, 26.09.2025.