

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 28.07.2026 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Нађа Никић под насловом „Имплементација Rabbit алгорита за шифровање“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Нађа Никић је рођена 21.02.2001. године у Новом Пазару. Завршила је основну школу „Сутјеска“ у Рашки као вуковац и ђак генерације. Уписала је гимназију у Рашки коју је завршила са одличним успехом. Електротехнички факултет уписала је 2019. године. Дипломирала је 2023. године на модулу Електроника. Дипломски рад одбранила је у септембру 2023. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на модулу Информационо комуникационе технологије уписала је у октобру 2025. године. Положила је све испите са просечном оценом 9,60.

2. Извештај о студијском истраживачком раду

Кандидат Нађа Никић је у склопу свог студијског истраживачког рада прво проучила релевантну литературу из области криптографије и сајбер безбедности. Проучила је типове заштите података и комуникације са посебним нагласком на алгоритме шифровања симетричним кључем. Потом је проучила блоковске и токовске алгоритме шифровања, и њихове предности и мане. Посебну пажњу је посветила алгоритму Rabbit за токовско шифровање. Детаљно је проучила спецификацију тог алгорита. Потом је осмислила архитектуру хардверске имплементације и извршила селекцију развојног окружења које би се користило у оквиру тезе. Изабрано је окружење ISE 14.7. Такође је извршена и селекција одговарајућег HDL језика за израду имплементације алгорита. Изабран је Verilog програмски језик. Након завршеног студијског истраживачког рада, Нађа је започела са израдом своје мастер тезе.

3. Опис мастер рада

Мастер рад обухвата 38 страна, са укупно 1 сликом, 7 табела и 8 референци. Рад садржи увод, 7 поглавља, закључак (укупно 9 поглавља), списак коришћене литературе, списак скраћеница, списак слика, списак табела и прилоге.

Уводно поглавље прво представља област којој припада тема да би потом били изложени предмет и циљ тезе. На крају је дат преглед организације остатка тезе.

Друго поглавље даје основе криптографије са посебним освртом на блоковске и токовске алгоритме шифровања симетричним кључем.

Треће поглавље додатно разматра токовске алгоритме шифровања симетричним кључем где је посебно разматрана улога кључева и иницијализационих вектора.

Четврто поглавље описује Rabbit алгорита за шифровање који је и предмет тезе. Описани су принцип рада алгорита и сви релевантни делови самог алгорита.

Пето и шесто поглавље описују саму имплементацију Rabbit алгорита. Прво је описана архитектура имплементације и генерални принцип рада са посебним освртом на реализовани коначни аутомат. Затим је детаљно описана имплементација при чему се темељно пролазило кроз све делове имплементације са одговарајућим објашњењима и исечцима кода ради лакшег разумевања и праћења датих објашњења. Описан је и део кода коришћен за верификацију реализоване имплементације Rabbit алгорита.

Седмо поглавље описује поступак верификације и представља резултате симулације. Имплементација је успешно верификована при чему су се користили тест вектори из спецификације алгорита.

Осмо поглавље кратко разматра безбедносне аспекте имплементације.

Девето поглавље резимира резултате тезе и даје смернице за наредна унапређења и проширења имплементације. Потом су дати списак референци, списак скраћеница, списак слика, списак табела и три прилога који садрже Verilog код имплементације и тест модула.

4. Анализа са кључним резултатима

Мастер рад Нађе Никић, дипл. инж. Електротехнике и рачунарства, је успешно имплементирао Rabbit

алгоритам за шифровање. Кључни доприноси рада кандидата на тези су следећи:

- 1) имплементиран Rabbit алгоритам за токовско шифровање;
- 2) реализована имплементација је портабилна и може да се користи на програмабилним чиповима различитих произвођача;
- 3) успешно верификована имплементација употребом тест вектора из спецификације алгоритма.

5. Закључак и предлог

Кандидат Нађа Никић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду имплементирала Rabbit алгоритам за шифровање у Verilog програмском језику. Нађа је показала висок степен знања из области дизајна комуникационог хардвера и способност да спецификације алгоритма преточи у хардверску архитектуру коју је потом и успешно реализовала. Резултати тезе могу да се користе у комуникационим уређајима за потребе шифровања комуникације, али и другим уређајима који имају сличну потребу. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Нађе Никић, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 09.09.2026. године

Чланови комисије:

др Зоран Чича Редовни професор
сагласан, 09.09.2026.

др Дејан Драјић Редовни професор
сагласан, 09.09.2026.

Алекса Стоименов Асистент
сагласан, 09.09.2026.