

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 23.06.2026 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Ива Барош под насловом „Хардверска имплементација ChaCha20 алгорита са шифровање“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Ива Барош је рођена 02.02.2000. године у Београду. Завршила је основну школу „Лазар Саветић“ у Београду као вуковац. Уписала је Земунску гимназију у Београду и коју је завршила са одличним успехом. Електротехнички факултет уписала је 2018. године. Дипломирала је на одсеку за Телекомуникације и информационе технологије 2023. године. 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 2023. године. Положила је све испите са просечном оценом 8,20.

2. Извештај о студијском истраживачком раду

Кандидат Ива Барош је у оквиру свог студијског истраживачког рада истражила релевантну литературу из области криптографије и криптографских алгоритама. Проучила је алгоритме шифровања симетричним кључем и архитектуре најпознатијих алгоритама. Потом је проучила блоковске и секвенцијалне алгоритме шифровања, и њихове разлике. Потом је пажњу посветила алгоритмима Salsa20 и ChaCha20 за секвенцијално шифровање. ChaCha20 јер је предмет тезе, а Salsa20 јер представља основу на којој је развијен поменути ChaCha20 алгоритам. Детаљно је проучила спецификације оба алгоритама. Осмислила је архитектуру хардверске имплементације и извршила избор развојног окружења које би се користило у оквиру тезе. Изабрано је окружење Intel Quartus Prime. Такође је извршена и селекција одговарајућег HDL језика за израду имплементације алгоритама. Изабран је VHDL програмски језик. Након завршеног студијског истраживачког рада, Ива је започела са израдом своје мастер тезе.

3. Опис мастер рада

Мастер рад обухвата 57 страна, са укупно 8 слика, 5 табела и 8 референци. Рад садржи увод, 5 поглавља, закључак (укупно 7 поглавља), списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Уводно поглавље указује на значај шифровања комуникације и алгоритама шифровања. Потом су наведени предмет и циљ тезе. На крају је дат преглед организације остатка тезе по поглављима.

Друго поглавље се бави симетричним алгоритмима шифровања са посебним освртом на секвенцијалне алгоритме којима припада и ChaCha20 алгоритам.

Треће поглавље представља Salsa20 алгоритам који је претеча ChaCha20 алгоритма. Описан је принцип рада Salsa20 алгоритма.

Четврто поглавље описује ChaCha20 алгоритам. Детаљно је описана структура алгоритма и свих појединачних компоненти. На крају су наведене карактеристике и предности ChaCha20 алгоритма. Пето поглавље детаљно описује имплементацију ChaCha20 алгоритма. Прво су описане архитектура имплементације и улога сваког од ентитета. Затим је детаљно описана имплементација свих градивних елемената. Одговарајући делови кода су дати уз опис имплементације ради лакшег разумевања датих објашњења.

Шесто поглавље описује начин верификације и представља добијене резултате симулације. Имплементација је успешно верификована при чему су се користили тест вектори из спецификације алгоритама. Такође је извршена процена заузећа ресурса и остварених перформанси за FPGA чип MAX 10 10M08DAF484C8G.

Седмо поглавље резимира резултате тезе и остварене перформансе имплементације. Потом су дати списак референци, списак скраћеница, списак слика и списак табела. Сам програмски код је приложен електронски.

4. Анализа са кључним резултатима

Мастер рад Иве Барош, дипл. инж. Електротехнике и рачунарства, је успешно имплементирао ChaCha20 секвенцијални алгоритам за шифровање. Кључни доприноси рада кандидата на тези су следећи:

- 1) имплементиран ChaCha20 алгоритам за секвенцијално 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;
- 4) извршена анализа перформанси реализоване имплементације.

5. Закључак и предлог

Кандидат Ива Барош, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду имплементирала ChaCha20 алгоритам за шифровање у VHDL програмском језику. Ива је показала способност да осмисли дизајн архитектуре и потом га ефикасно и брзо реализује, али и квалитетног презентовања својих резултата тако да буду разумљиви широј публици. Резултати тезе могу да се користе у мрежним уређајима за потребе заштите комуникације у мрежи, али и у другим уређајима који имају сличну потребу. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Иве Барош, 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.