

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 04.06.2024 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Мина Каљевић под насловом „Имплементација SNOW 3G алгоритма за шифровање“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Мина Каљевић је рођена 03.08.1999. године у Чачку. Завршила је Основну школу „Милица Павловић“ у Чачку као вуковац. Уписала је Гимназију у Чачку коју је такође завршила као вуковац. Током школовања освојила је више првих награда на општинским и окружним такмичењима из математике, физике, српског језика и различитих спортова (одбојка, рукомет, кошарка, стрељаштво, атлетика). Електротехнички факултет уписала је 2018. године. Дипломирала је на одсеку за Телекомуникације и информационе технологије 2022. године са просечном оценом 7,89. Дипломски рад одбранила је у септембру 2022. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на модулу за Информационо комуникационе технологије уписала је у октобру 2022. године. Положила је све испите са просечном оценом 7,80.

2. Извештај о студијском истраживачком раду

Кандидат Мина Каљевић је у оквиру свог студијског истраживачког рада проучила област криптографије са посебним освртом на стрим алгоритме шифровања. Првенствено се посветила SNOW 3G алгоритму који је и предмет мастер тезе. Поред тога, проучила је развојна окружења која могу да се користе за VHDL дизајн и симулацију пошто је циљ мастер тезе хардверска имплементација SNOW 3G алгоритма употребом VHDL језика. Након урађеног студијског истраживачког рада, Мина је започела израду своје мастер тезе.

3. Опис мастер рада

Мастер рад обухвата 42 стране, са укупно 21 сликом и 17 референци. Рад садржи увод, 3 поглавља, закључак (укупно 5 поглавља), списак коришћене литературе, списак скраћеница и списак слика. У уводном поглављу је наглашен значај безбедности у модерним комуникацијама. Изложени су основни подаци SNOW 3G алгоритма за шифровање који представља предмет тезе. На крају је изложен циљ саме тезе.

Друго поглавље даје кратак преглед историјата и значаја криптографије у мобилним мрежама пошто се SNOW 3G алгоритам првенствено користи у тим мрежама.

Треће поглавље даје веома детаљан опис SNOW 3G алгоритма. Изложен је опис структуре самог алгоритма, као и принцип рада. Поред тога, анализирана је временска и просторна сложеност алгоритма, као и његова безбедност и ограничења.

Четврто поглавље садржи опис реализоване хардверске имплементације SNOW 3G алгоритма. Коришћен је VHDL програмски језик, и уз опис дизајна су дати делови реализованог кода. На крају је описана верификација реализованог дизајна која је потврдила исправност реализације.

Пето поглавље резимира резултате мастер тезе и даје смернице за будућа унапређења реализоване имплементације. Потом су дати списак референци, списак скраћеница и списак слика.

4. Анализа са кључним резултатима

Мастер рад Мине Каљевић, дипл. инж. Електротехнике и рачунарства, представља хардверску имплементацију SNOW 3G алгоритма за стрим шифровање. Кључни доприноси рада кандидата на тези су следећи:

- 1) реализована имплементација SNOW 3G 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 Мина Каљевић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно реализовала хардверску имплементацију SNOW 3G алгоритма за стрим шифровање. Реализована имплементација се може користити у комуникационим уређајима за шифровање комуникације. Мина је показала способност да самостално проучи један алгоритам за шифровање и да потом на основу спецификације креира одговарајући хардверски дизајн. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Мине Каљевић, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 03.10.2025. године

Чланови комисије:

др Зоран Чича Редовни професор
сагласан, 03.10.2025.

др Дејан Драјић Редовни професор
сагласан, 03.10.2025.