

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 26.08.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Вукашин Драговић под насловом „Имплементација blockchain-а заснованог на пост-квантним алгоритмима енкрипције“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Вукашин Драговић је рођен 04.07.2000. године у Београду. Завршио је основну школу „Јован Дучић“ у Београду као вуковац. Уписао је Девету београдску гимназију у Београду коју је завршио са одличним успехом. Електротехнички факултет уписао је 2019. године. Дипломирао је на одсеку за Софтверско инжењерство 2023. године са просечном оценом 9,58. Дипломски рад одбранио је у септембру 2023. године са оценом 10. Мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство уписао је у октобру 2023. године. Положио је све испите на мастер студијама са просечном оценом 9.60. У току основних студија обавио је праксу у компанији Microsoft, где од јула 2023. године ради као софтвер инжењер.

2. Извештај о студијском истраживачком раду

Кандидат Вукашин Драговић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на blockchain системе, квантне рачунаре и пост-квантне алгоритме енкрипције. Конкретно, анализирана су постојећа решења и проблеми у области blockchain система, као и проблематика постојећих алгорита енкрипције који нису отпорни на квантне рачунаре. Истраживањем области утврђено је да најпознатија решења blockchain криптовалута не користе пост-квантне алгоритме енкрипције, што значи да су ти системи рањиви на квантне рачунаре, посебно уз интензиван развој квантних рачунара у последњим годинама.

3. Опис мастер рада

Мастер рад обухвата 38 страна не укључујући насловну страну и садржај, са укупно 15 слика, 5 табела и 12 референци. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак слика и списак табела.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљени су концепти blockchain-а, дат је увид у алгоритме енкрипције који се користе у тренутним blockchain системима, и изнесен је проблем развоја квантних рачунара и њихов утицај на постојеће алгоритме.

У другом поглављу је дат кратак преглед технологије blockchain-а, класичних алгорита енкрипције и квантних рачунара. Детаљније је објашњен утицај квантних рачунара на класичне алгоритме енкрипције. У трећем поглављу су детаљно представљени пост-квантни алгоритми за шифровање и дигитално потписивање као решење проблема рањивости класичних криптографских алгорита. Алгоритми који су описани у овом поглављу су Kyber и Dilithium, који су недавно стандардизовани и прихваћени за употребу. Четврто поглавље детаљно описује имплементирани систем са функционалним карактеристикама свих имплементираних апликација.

У оквиру петог поглавља је описана спроведена анализа перформанси коришћених алгорита у имплементацији система, и анализирани су кључни изазови у преласку са класичних алгорита енкрипције на пост-квантне.

Шесто поглавље је закључак у оквиру кога је резимирано имплементирано решење, дат закључак о утицају пост-квантних алгорита и предложени могући кораци за унапређење имплементираног система.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Вукашина Драговића се бави проблемом пројектовања и реализације blockchain система заснованог на пост-квантним алгоритмима енкрипције. С обзиром на чињеницу да се инвестира у развој квантних рачунара, прелазак на алгоритме који су отпорни на овај тип рачунара је од изузетног значаја. У склопу рада су описане предности и мане преласка на пост-квантне алгоритме. Имплементирано решење је тестирано у оквиру једног рачунара, а уз даље развијање могуће је проширити да систем

функционише на више рачунара истовремено.

Основни доприноси рада су: 1) приказ и методологија пројектовања blockchain система; 2) анализа утицаја класичних и пост-квантних алгоритама на blockchain; 3) могућност даљег развоја имплементираног blockchain прототипа.

5. Закључак и предлог

Кандидат Вукашин Драговић је у свом мастер раду успешно решио проблем пројектовања и имплементације прототипа blockchain система са и без коришћења пост-квантних алгоритама енкрипције, извршио анализу коришћених алгоритама и њиховог утицаја на систем. Кандидат је дао закључак о проблематици коришћења пост-квантних алгоритама у постојећим blockchain системима.

Кандидат је исказао самосталност и систематичност у своме поступку као и иновативне елементе у решавању проблематике овог рада.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Вукашина Драговића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 16.10.2025. године

Чланови комисије:

др Павле Вулетић Редовни професор
сагласан, 16.10.2025.

др Жарко Станисављевић Ванредни
професор
сагласан, 16.10.2025.