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. Јован Јаковљевић под насловом „Анализа принципа и безбедносних аспеката квантне криптографије". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Јован Јаковљевић је рођен 7. 6. 2000. године у Крагујевцу. Завршио је основну школу „Станислав Сремчевић“ у Крагујевцу као вуковац. Уписао је Прву крагујевачку гимназију коју је завршио са одличним успехом. Током школовања освојио је прву награду на окружном такмичењу из биологије у 2. години. Електротехнички факултет је уписао 2019. године. Дипломирао је на одсеку Физичка електроника са просечном оценом 8,33. Дипломски рад на тему „Месбауереве спектроскопије“ је одбранио у септембру 2024. са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за биомедицинско и еколошко инжењерство, уписао је у октобру 2024. године. Положио је све испите са просечном оценом 7,40.

2. Извештај о студијском истраживачком раду

Кандидат Јован Јаковљевић је као припрему за израду мастер рада обавио истраживање релевантне литературе која се односи на област којој припада тема мастер рада. Конкретно, анализирана су постојећа решења и проблеми у области класичне и квантне криптографије. Истраживањем је утврђено да класични алгоритми имају велике слабости у смислу да су одређени квантни алгоритми теоријски у стању да дешифрују поруке које се преносе класичним путем. У раду су анализирани протоколи за квантни пренос информација и упоређени са најсавременијим класичним криптографским методама. Установљено је да квантне комуникације представљају солидну алтернативу која у догледној будућности може да обезбеди тајност комуникација.

3. Опис мастер рада

Мастер рад обухвата 37 страна (од чега прилог са кодом обухвата 6 страна), не рачунајући насловну страну и садржај, са укупно 11 слика, 2 табеле и 6 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 поглавља), списак скраћеница, слика, табела и коришћене литературе.

Прво поглавље представља уводни део рада, у којем су дефинисани предмет и циљ рада. Изложене су основе квантног рачунања, са посебним освртом на његов потенцијални утицај на безбедност савремених класичних комуникационих протокола.

У другом поглављу је дат кратак преглед основних протокола за безбедну размену информација. Објашњена је улога квантних рачунара у разбијању неких од најзаступљенијих криптосистема данашњице, као и модификације класичних алгоритама које у одређеној мери могу да умање опасност од савремених квантних система.

У трећем поглављу су представљени принципи квантне криптографије. Дат је кратак историјат и детаљно је анализирана квантна дистрибуција кључа на примеру ББ84 протокола. Имплементација је реализована путем емулације кода написаног у програму Пајтон и уз помоћ библиотеке Qiskit. Главни резултати су приказани табеларно. Детаљно су анализирани: модел ограниченог и бучног квантног складиштења, квантна криптографија у случају неповерења, квантна криптографија базирана на позицији и квантна криптографија независна од уређаја.

Четврто поглавље обухвата анализу безбедности квантне дистрибуције кључа, као и основе постквантне криптографије, чији је циљ обезбеђивање отпорности на квантне нападе. Такође, извршена је компаративна анализа модификованих класичних алгоритама са повећаном отпорношћу на квантне нападе и квантних алгоритама.

Пето поглавље представља закључак рада, у оквиру којег је разматран значај квантних решења за унапређење безбедности комуникација, као и потенцијал квантних рачунара да угрозе безбедност класичних комуникационих алгоритама. Сажети су главни резултати рада и размотрени изазови повезани са тренутним степеном развоја квантних система.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Јована Јаковљевића се бави савременом проблематиком квантних комуникација. Тренутни степен развоја квантних рачунара још увек није на нивоу који би омогућио угрожавање безбедности класичних комуникационих система, док квантне комуникације пружају могућност остваривања вишег нивоа безбедности и тајности преноса података у односу на постојеће комуникационе системе. Убрзан развој квантног хардвера указује на могућност да квантни рачунари у блиској будућности постану способни да угрозе безбедност појединих класичних криптографских алгоритама, због чега би примена квантних комуникационих система могла постати значајна за обезбеђивање сигурног преноса информација.

Имплементација постојећег квантног протокола за комуникацију кроз програмски код и емулација у локалном окружењу верификује велику безбедност квантних комуникационих система.

Основни резултати рада су: 1) систематичан преглед савремених класичних и квантних криптографских алгоритама; 2) имплементација и верификација поузданости изабраног квантног алгоритма за комуникацију; 3) могућност наставка рада на развоју квантних алгоритама и модификацију класичних тако да остану довољно безбедни на квантне претње.

5. Закључак и предлог

Кандидат Јован Јаковљевић је у свом мастер раду успешно размотрио предности и проблеме квантних комуникација. Детаљно је анализирао ефикасност ових алгоритама у смислу тренутног степена развоја квантних система. Указао је на могућност адаптације класичних алгоритама тако да буду мање подложни на квантне нападе. Своје тврдње је верификовао путем емулације програмског кода у локалном окружењу. Урађена анализа може бити од велике користи у смислу смерница за даљи развој квантних и класичних криптографских алгоритама..

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. Јована Јаковљевића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 11.09.2026. године

Чланови комисије:

др Владимир Арсоски Редовни професор
сагласан, 11.09.2026.

др Милан Тадић Редовни професор
сагласан, 11.09.2026.