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. Лука Милићевић под насловом „Софтверска имплементација проактивног дистрибуираног система за управљање кључевима применом шема дељења тајне". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Лука Милићевић је рођен 04.08.2001. године у Ваљеву. Завршио је основну школу „Драгољуб Илић" у Драчићу. Уписао је Гимназију у Ваљеву 2016. године, природно-математички смер. Електротехнички факултет је уписао 2020. године. Дипломирао је са просечном оценом 8,53 на одсеку за Телекомуникације и информационе технологије. Дипломски рад из предмета Усмерене радио везе, на тему „Развој софтвера за прорачун интерференције у радио релејним мрежама", одбранио је 2024. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за информационо комуникационе технологије, уписао је у октобру 2024. године. Положио је све испите са просечном оценом 9,80. Запослен је од септембра 2024. године.

2. Извештај о студијском истраживачком раду

Кандидат Лука Милићевић је као припрему за израду мастер рада урадио преглед релевантне литературе која се односи на технике заштите поверљивих података у савременим дистрибуираним системима, са тежиштем на праговној криптографији и дељењу тајне. Познато је да чување главних (мастер) кључева на једном месту уводи јединствену тачку отказа: тајна се тиме чини поверљивом, али и крхком, док њено умножавање ради поузданости повећава број мета за напад. Дељење тајне овај проблем решава расподелом тајне на више носилаца тако да само довољан број учесника заједно може да је реконструише. Предмет рада представља обједињавање четири класичне шеме дељења тајне Шамирове шеме, Фелдманове шеме проверивог дељења, Херзбергов модела проактивног дељења и протокола CHURP за динамичке комитете у јединствено развојно окружење и њихову експерименталну проверу. За неколико практично значајних сценарија извршена је процена рачунског и комуникационог трошка у зависности од броја чворова и безбедносног прага реконструкције. За реализацију развојног окружења, асинхроног мрежног симулатора и анализу резултата коришћен је програмски језик Python.

3. Опис мастер рада

Мастер рад обухвата 34 стране, са укупно 8 слика и 1 табелом. Рад садржи увод, шест поглавља и закључак (укупно 8 поглавља), списак литературе, списак скраћеница, списак слика и списак табела.
Прво поглавље представља увод у коме су описани предмет и циљ рада, значај дистрибуираног управљања кључевима, као и допринос рада. Друго поглавље излаже математичку основу Шамировог дељења тајне: мотивацију за настанак шеме, разлоге за примену аритметике над пољем Галоа, употребу полинома, поступке прављења и реконструкције тајне, безбедносна својства и недостатке основне шеме. У трећем поглављу описано је проактивно дељење тајне и Херзбергов модел, укључујући модел нападача у покрету и појам епоха, фазу освежавања кључева, обнављање и регенерацију делова тајне, као и прелаз од статичких ка динамичким комитетима. У четвртом поглављу представљено је Фелдманово провериво дељење тајне: криптографска основа, хомоморфни комитменти, поступак верификације исправности удела, као и позитивне и негативне стране провере.
Пето поглавље описује динамичке комитете и протокол CHURP, укључујући асиметрични биваријантни полином, пуне и редуковане делове, примопредају тајне, ефикасно нула-дељење са две променљиве, полиномске комитменте и различите типове CHURP конструкције. У шестом поглављу објашњени су дизајн и имплементација развојног окружења. Седмо поглавље садржи експерименталне резултате: мерење рачунског трошка дељења и реконструкције, комуникационог трошка примопредаје у зависности од броја чворова и од прага, стабилности и исправности током више епоха, као и понашања система у присуству напада и отказа, што представља главни резултат рада. У закључку је дат осврт на рад са нагласком на допринос обједињавања шема и правце за даље истраживање. Потом су дати списак коришћених

референци, списак скраћеница, списак слика и списак табела.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Луке Милићевића бави се пројектовањем, имплементацијом и анализом проактивног дистрибуираног система за управљање кључевима заснованог на дељењу тајне са динамичким комитетима. Полазни проблем је јединствена тачка отказа при чувању кључева високе вредности, који се разрешава низом криптографских шема при чему свака уклања по једно ограничење претходне: Шамирова шема поставља основу дељења тајне, Фелдманова шема додаје проверу исправности удела и откривање преваре, Херзбергов проактивни модел уводи обнављање удела кроз епохе, а протокол CHURP проширује проактивно дељење на динамичке комитете. Све шеме повезане су заједничком идејом освежавања удела додавањем „поделе нуле", која мења сваки удео не мењајући саму тајну.

Практични део рада реализује овај низ шема у облику слојевитог софтверског оквира написаног у језику Python, са асинхроним мрежним симулатором за мерење комуникационог трошка. Резултати показују да је рачунски трошак низак и сагласан са очекиваном сложеношћу Лагранжове интерполације при највећем испитаном броју чворова ($n = 160$, $t = 79$) комплетно дељење и реконструкција трају око осам милисекунди — те да главни трошак система лежи у комуникацији током примопредаје. Потврђено је да је тајна очувана кроз двадесет узастопних епоха уз стабилан и предвидив трошак по епохи, као и да систем поуздано открива покварене уделе, непоштеног делиоца, пад чвора и покушај кршења прага. Посебно је вредан налаз да наивна проактивизација достиже сложеност реда $O(n^4)$, чиме се оправдава постојање ефикасног дводимензионог дељења нуле у пуном CHURP протоколу.

5. Закључак и предлог

Кандидат Лука Милићевић је у свом мастер раду успешно објединио четири класичне шеме за дељење тајне у јединствен, функционалан софтверски оквир и експериментално оценио његове перформансе. Систем је анализиран у погледу рачунског и комуникационог трошка за различите бројеве чворова и прагове реконструкције, а описане су главне предности и ограничења примењених шема. Лука је показао да добро влада материјом коју је описао у раду и исказао самосталност у пројектовању архитектуре и писању програмског кода који је коришћен за добијање нумеричких резултата.
На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Луке Милићевића прихвати као мастер рад и да се кандидату одобри јавна усмена одбрана.

Београд, 28.08.2026. године

Чланови комисије:

др Предраг Иваниш Редовни професор
сагласан, 28.08.2026.

др Зоран Чича Редовни професор
сагласан, 28.08.2026.