

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Реферат о урађеној докторској дисертацији кандидата Марка Мићовића 2018/5013, мастер инжењера електротехнике и рачунарства

Одлуком бр. 480/28 од 10.03.2026. године, именовани смо за чланове Комисије за преглед, оцену и одбрану докторске дисертације кандидата Марка Мићовића бр. индекса 2018/5013 под насловом

Заштита приватности на мрежном слоју применом шифровања са очувањем формата

(енгл. *Network layer privacy protection using format preserving encryption*)

После прегледа достављене дисертације и других пратећих материјала и разговора са кандидатом, Комисија је сачинила следећи

РЕФЕРАТ

1. УВОД

1.1. Хронологија одобравања и израде дисертације

Докторске академске студије на Електротехничком факултету Универзитета у Београду, на модулу за Рачунарску технику и информатику, кандидат Марко Мићовић је уписао у октобру 2018. године. Кандидат је положио све испите са оценом 10 и остварио 120 ЕСПБ. Такође, испунио је све обавезе везане за студијски истраживачки рад које су предвиђене наставним планом и програмом докторских студија. Кандидат је 22.12.2023. пријавио тему за израду докторске дисертације под насловом „Заштита приватности на мрежном слоју применом шифровања са очувањем формата” Катедри за рачунарску технику и информатику на Електротехничком факултету Универзитета у Београду.

Катедра за рачунарску технику и информатику, на својој седници одржаној дана 26.12.2023. године, размотрила је пријаву теме докторске дисертације коју је поднео кандидат. Катедра је утврдила да је надлежна за разматрање пријављене теме докторске дисертације, као и да су достављена пријава и њени прилози суштински и формално одговарајући и комплетни.

Комисија за студије трећег степена Електротехничког факултета Универзитета у Београду је на својој седници одржаној дана 09.01.2024. године разматрала пријаву теме за израду докторске дисертације и предлог састава Комисије за оцену научне заснованости теме докторске дисертације. Комисија за студије трећег степена је пријаву теме и предлог састава Комисије за оцену научне заснованости теме докторске дисертације упутила Наставно-научном већу Електротехничког факултета Универзитета у Београду на усвајање.

Наставно-научно веће Електротехничког факултета Универзитета у Београду је, на својој 893. седници одржаној дана 16.01.2024. године, донело одлуку бр. 75-30 о именовану Комисије за оцену научне заснованости теме докторске дисертације у саставу:

- др Захарије Радивојевић, ванредни професор
Електротехнички факултет Универзитета у Београду
- др Дејан Симић, редовни професор
Факултет организационих наука, Универзитета у Београду
- др Зоран Чича, редовни професор
Електротехнички факултет Универзитета у Београду

За ментора је предложен др Павле Вулетић, редовни професор Електротехничког факултета Универзитета у Београду.

Јавна усмена одбрана теме докторске дисертације је одржана дана 24.01.2024. године. Комисија за оцену научне заснованости теме докторске дисертације оценила је усмену одбрану као успешну (оцена „задовољио“).

Комисија за студије трећег степена Електротехничког факултета Универзитета у Београду је на својој седници која је одржана дана 13.02.2024. године разматрала записник Комисије за оцену научне заснованости теме докторске дисертације са јавне усмене одбране, који је упутила Наставно-научном већу Електротехничког факултета Универзитета у Београду на усвајање.

Наставно-научно веће Електротехничког факултета Универзитета у Београду је, на својој 894. седници одржаној дана 20.02.2024. године, усвојило извештај Комисије за оцену научне заснованости теме докторске дисертације кандидата, а за ментора је именован др Павле Вулетић, редовни професор Електротехничког факултета Универзитета у Београду.

Веће научних области техничких наука Универзитета у Београду је, на својој седници одржаној дана 18.03.2024. године, дало сагласност на предложену тему докторске дисертације и именовање ментора (број одлуке 61206-859/2-24).

Кандидат је предао докторску дисертацију на преглед и оцену 23.02.2026. године.

Комисија за студије трећег степена Електротехничког факултета Универзитета у Београду је, на седници одржаној дана 03.03.2026. године, потврдила испуњеност потребних услова за подношење предлога Наставно-научном већу Електротехничког факултета Универзитета у Београду за формирање Комисије за оцену докторске дисертације.

Наставно-научно веће Електротехничког факултета Универзитета у Београду је, на својој 926. седници одржаној дана 10.03.2026. године, именovalo Комисију за оцену докторске дисертације у саставу:

- др Захарије Радивојевић, ванредни професор
Електротехнички факултет Универзитета у Београду
- др Зоран Чича, редовни професор
Електротехнички факултет Универзитета у Београду
- др Дејан Симић, редовни професор
Факултет организационих наука Универзитета у Београду
- др Милош Цветановић, ванредни професор
Електротехнички факултет Универзитета у Београду
- др Саша Стојановић, ванредни професор
Електротехнички факултет Универзитета у Београду

На основу члана 101. Статута Универзитета у Београду, члана 74. Статута Електротехничког факултета Универзитета у Београду и захтева студента, одобрено је продужење рока за завршетак студија до истека троструког броја школских година потребних за реализацију уписаног студијског програма.

1.2. Научна област дисертације

Дисертација припада научној области Електротехника и рачунарство, а ужа научна област дисертације је Рачунарска техника и информатика, док у оквиру уже научне области припада области Рачунарских мрежа. Ментор дисертације је др Павле Вулетић, редовни професор Електротехничког факултета Универзитета у Београду, који има доприносе у наставном и научном раду у области Рачунарских мрежа.

1.3. Биографски подаци о кандидату

Марко Мићовић рођен је 3. јула 1993. године у Београду. Основну школу „Стеван Синђелић” завршио је као носилац Вукове дипломе. Трећу београдску гимназију, на природно-математичком смеру, завршио је са одличним успехом.

Основне академске студије на Електротехничком факултету у Београду, на одсеку Електротехника и рачунарство, уписао је 2012. године. Основне академске студије на модулу Рачунарска техника и информатика завршио је 2016. године са просечном оценом 9,04. Дипломски рад на тему „Систем за идентификацију студената употребом бесконтактних картица” под менторством ванредног професора др Милоша Цветановића одбранио је са оценом 10. Током основних студија био је на стручној пракси у фирми „Микроелектроника”.

Мастер академске студије на Електротехничком факултету у Београду уписао је 2016. године. Мастер академске студије на модулу Рачунарска техника и информатика завршио је 2018. године са просечном оценом 10. Мастер рад на тему „Окружење за прикупљање информација о извршавању програма” под менторством ванредног професора др Саше Стојановића одбранио је са оценом 10.

Докторске академске студије на Електротехничком факултету у Београду уписао је 2018. године на модулу Рачунарска техника и информатика. Положио је све испите са просечном оценом 10. У истраживачком раду оријентисао се ка областима уграђених уређаја и рачунарских мрежа. Похађао је летњу школу *ACACES (Advanced Computer Architecture and Compilation for High-performance Embedded Systems)* 2019. године. Током мастер и докторских академских студија има објављена 2 научна рада у часопису са *SCI* листе, 9 научних радова на страним конференцијама и 11 научних радова на домаћим конференцијама као аутор или коаутор.

Почев од децембра 2016. године запослен је на Електротехничком факултету у Београду. У периоду од 2016. до 2018. године био је изабран у звање сарадник у настави. Почев од 2018. године запослен је као асистент на истом факултету и тренутно је ангажован на предметима: Рачунарске мреже 1, Рачунарске мреже 2, Микропроцесорски системи, Оперативни системи 1, Системски софтвер и Програмирање мобилних уређаја. Био је на стручном усавршавању у фирми „*Elsys Eastern Europe*”.

За време периода у току којег је запослен на Електротехничком факултету учествује на више комерцијалних пројеката. Учествовао је као предавач у програму преквалификација у области информационих технологија који је организовао Развојни програм Уједињених нација током 2019, 2021, 2022. године. Сарађивао је у склопу комерцијалних пројеката са неколико фирми као и колегама са других катедри Електротехничког факултета. Најистакнутији такав пројекат јесте „Развој и реализација софтвера за прорачун звучне изолације” у сарадњи са фирмом „*URSA*”. Учесник је или је био учесник на неколико научних пројеката: 1) „Развој дигиталних технологија и умрежених сервиса у системима са

уграђеним електронским компонентама” који финансира Министарство просвете, науке и технолошког развоја, 2) „Иновација групе предмета из области рачунарских мрежа, интернета и заштите података”, 3) „УНАР - Унапређење наставе из Архитектуре рачунара” које је финансирало Министарство просвете, науке и технолошког развоја, 4) „*Advancing novel textual similarity-based solutions in software development (AVANTES)*” који је финансирао Фонд за науку Републике Србије, 5) „*Belgrade Data Innovation Hub (BELDIH)*” - HORIZON 2020 и 6) „*Software for Text Offenses Prevention in Serbian: AI-driven Hate Speech Detection (STOP)*” који је финансирао Фонд за науку Републике Србије.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1. Садржај дисертације

Дисертација је написана на српском језику ћириличним писмом и има 145 страна од чега је 104 нумерисано. Дисертација садржи 44 слике, 8 табела, 9 алгоритама и 4 исечка са програмским кодом. Дисертација је подељена на 8 поглавља:

1. Увод
2. Проблем заштите приватности
3. Шифровање са очувањем формата
4. Архитектура *LISPP* система
5. Имплементација *LISPP* система
6. Евалуација *LISPP* система
7. Примена *LISPP* система
8. Закључак

Додатно дисертација садржи и насловне стране на српском и енглеском језику, страну са информацијама о ментору и члановима комисије за оцену, захвалницу, сажетак на српском и енглеском језику, садржај, списак слика, списак табела, списак литературе са 172 референце наведене по редоследу појављивања у тексту, три прилога (исечци кода хардверске и софтверске имплементације *LISPP* система, значајни делови *DNS* лога), биографију аутора и потребне изјаве (о ауторству, о истоветности штампане и електронске верзије докторског рада и о коришћењу).

2.2. Кратак приказ појединачних поглавља

Прво поглавље представља увод ове дисертације. У оквиру овог поглавља представљен је кратки осврт на проблем заштите приватности корисника на интернету, која је угрожена на различите начине и на неколико слојева *OSI* модела, уз фокус на прикупљање података и профилисање на мрежном слоју. Изложене су полазне хипотезе уз истицање да постојећи механизми заштите приватности на мрежном слоју неретко нарушавају перформансе мреже због ослањања на класичне алгоритме шифровања и потребе за чувањем стања система. Као одговор на ове изазове, представљен је *LISPP (Lightweight Stateless Privacy Protection)* систем у оквиру којег се по први пут користе алгоритми шифровања са очувањем формата за ефикасно замагљивање делова заглавља пакета попут *IP* адреса. На крају, дат је преглед структуре комплетне дисертације.

Друго поглавље детаљно разматра изазове заштите приватности корисника, почев од апликативног слоја где су анализирани механизми праћења путем колачића и јединствених дигиталних отисака веб прегледача. Затим је анализирана заштита веб комуникације, при чему су истакнута ограничења постојећих решења, попут *Tor* система, пре свега у погледу повећаног кашњења и деградације перформанси. Након тога, главни фокус је стављен на мрежни слој, те су представљене конкретне предности програмабилних мрежних уређаја у контексту брже и ефикасније обраде саобраћаја. Највећи и најзначајнији део овог поглавља

чини систематична свеобухватna компаративna анализа постојећих система за заштиту приватности на мрежном слоју. Приказана су решења развијена у различитим периодима, закључно са најмодернијим која користе предности програмабилних мрежних уређаја. Систематизацијом ових решења на она са јаким и релаксираним гаранцијама заштите приватности, прецизно су сумиране њихове главне предности и недостаци.

Треће поглавље елаборира потребу примене алгоритама шифровања са очувањем формата у контексту заштите приватности на мрежном слоју. Указано је на неадекватност класичних блоковских алгоритама за ову сврху, с обзиром на то да они најчешће захтевају проширивање кратких поља заглавља пакета, што нарушава формат самог пакета и изискује додатно чување проширених шифрованих података. Као решење предложено је шифровање са очувањем формата захваљујући којем се избегава потреба за изменом формата пакета. Детаљно су представљена два скупа стандардизованих алгоритама заснованих на Фајстеловој структури: алгоритми *FF1* и *FF3-1*, које препоручује амерички *NIST*, као и алгоритми *FEA-1* и *FEA-2*, који су стандардизовани од стране корејског *KATS*. Закључни део поглавља посвећен је алгоритму *FF3-1*, који је изабран као основа за предложени *LISPP* систем због мањег броја рунди и прикладних ограничења за величину домена улазних података.

У четвртном поглављу детаљно је представљена архитектура предложеног *LISPP* система намењеног заштити приватности на мрежном слоју без потребе за чувањем стања сесија. Описан је процес замагљивања података о кориснику, шифровањем хост дела изворишне *IP* адресе и изворишног порта применом алгоритама шифровања са очувањем формата на самој граници заштићене мреже. Истакнуто је да *LISPP* систем омогућава транспарентан рад за крајње кориснике, независан је од протокола што значи да подржава обе верзије интернет протокола, при чему смањује ризик од профилисања корисника. Као додатни позитиван ефекат, уочено је и отежано извођење скенирања портова, чиме се уједно повећава укупна безбедност мреже. На самом крају анализирани су изазови приликом ажурирања криптографског материјала, с обзиром на то да промена кључева захтева пажљиво планирање како би се избегао прекид активних корисничких сесија.

Пето поглавље детаљно излаже најбитније детаље имплементације *LISPP* система кроз примену технологија за програмирање равни података, које омогућавају флексибилну модификацију мрежних пакета без нарушавања перформанси обраде. Иницијално је размотрен развој концепта софтверски дефинисаних мрежа, програмабилне равни података и програмабилних мрежних уређаја, са посебним фокусом на предности *P4* језика и *eBPF* технологије у контексту брзог и безбедног пресретања саобраћаја. На основу тога, представљена је хардверска имплементација система прилагођена *Netronome SmartNIC* уређајима, која се ослања на *P4* и *Micro-C* језик за постизање максималног пропусног опсега. Као алтернатива, развијена је и детаљно описана софтверска верзија заснована на *eBPF* технологији и *XDPA* прикључцима, чиме је омогућена интеграција система директно у језгро Линукс оперативног система у циљу шире примене.

У шестом поглављу извршена је експериментална евалуација предложеног *LISPP* система кроз мерења пропусног опсега, протока пакета и додатног кашњења. Детаљно су приказани резултати тестирања на *Netronome SmartNIC* уређају, при чему је установљено да су оптималне перформансе постигнуте имплементацијом заснованом на *Micro-C* језику. Такође, испитана је могућност оптимизације перформанси кроз смањење броја *AES* рунди у оквиру сваке рунде *FF3-1* алгоритма, чиме је омогућен осетно већи проток пакета. Поред тога, спроведена су тестирања *eBPF* софтверске имплементације у виртуелном окружењу, током којих су забележена минимална и конзистентна кашњења независно од величине пакета. Кроз све представљене анализе потврђено је да је *LISPP* систем ефикасан, скалабилан и применљив у реалним мрежним окружењима при великим брзинама.

Седмо поглавље излаже детаљну анализу примене предложеног *LISPP* система за заштиту приватности у оквиру *DNS* сервиса. Након прегледа постојећих безбедносних механизма, дефинисан је *LDoH (LISPP DoH)* сервис којим је омогућена анонимизација клијената. Заштита идентитета је остварена замагљивањем изворишних *IP* адреса, чиме је успешно избегнута потреба за успостављањем вишеструких *TLS* сесија. Кроз спроведену експерименталну евалуацију доказано је да су предложеним приступом остварене боље перформансе и мања кашњења у поређењу са алтернативним *ODoH* сервисом. На крају, на основу анализе реалног мрежног саобраћаја, размотрена је и предложена оптимална стратегија за ротацију криптографског материјала током рада система.

Осмо поглавље представља закључак ове дисертације. У овом поглављу су сумирани кључни доприноси дисертације, чиме је потврђена ефикасност примене алгоритама за шифровање са очувањем формата у сврху заштите приватности на мрежном слоју. Показано је да су мане класичних блоковских алгоритама успешно превазиђене развојем *LISPP* система, чиме је омогућено потпуно транспарентно замагљивање *IP* адреса без нарушавања стандардног формата пакета. Употребљивост предложеног решења је доказана кроз имплементацију за програмабилну мрежну картицу, као и кроз извршавање унутар језгра Линукс оперативног система коришћењем *eBPF* технологије. Такође, перформансе *LISPP* система су директно демонстриране евалуацијом *LDoH* сервиса, при чему су остварене боље перформансе приликом заштите *DNS* саобраћаја у поређењу са постојећим решењима која пружају еквивалентан ниво заштите приватности. На самом крају, јасно су дефинисани правци за даља истраживања којима су обухваћене додатне оптимизације перформанси, подршка за нове алгоритме и проширење примене на друге мрежне протоколе.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1. Савременост и оригиналност

Имајући у виду да је заштита приватности на интернету препозната као један од великих изазова данашњице, као и да њено компромитовање може изазвати озбиљне последице, савременост и релевантност ове дисертације су недвосмислено потврђене. Праћење корисника путем анализе заглавља пакета, посебно изложене *IP* адресе, је идентификовано као критична рањивост чије решавање захтева посебну пажњу. Актуелност истраживања додатно је наглашена употребом најсавременијих мрежних технологија у процесу имплементације предложених решења. Конкретно, предложени концепти су успешно имплементирани и евалуирани на програмабилној мрежној картици коришћењем *P4* језика, као и коришћењем *eBPF* технологије унутар језгра Линукс оперативног система. На овај начин је доказано да модерни трендови у развоју мрежних инфраструктура могу бити ефикасно искоришћени за постизање високих перформанси приликом заштите приватности.

Научни допринос ове дисертације у погледу оригиналности огледа се у пионирској примени алгоритама за шифровање са очувањем формата директно на мрежном слоју, у циљу анонимизације података који идентификују корисника. За разлику од постојећих решења за заштиту приватности на мрежном слоју, која се превасходно засновају на традиционалном блоковском шифровању, ова дисертација по први пут предлаже употребу шифровања са очувањем формата у поменутом контексту. Захваљујући овом оригиналном приступу, успешно је избегнуто нарушавања стандардног формата пакета и омогућена је анонимизација идентификационих података без промене дужине заглавља. Истовремено је у потпуности елиминисана и потреба за комплексним праћењем стања активних сесија, што је до сада представљало изражен недостатак у погледу мрежних перформанси. Сходно томе, предложени *LISPP* систем представља решење које елегантно премошћује теоријска и практична ограничења већине постојећих механизма.

3.2. Осврт на референтну и коришћену литературу

У дисертацији је наведено укупно 172 референце које су нумерисане према редоследу појављивања у тексту. Референце обухватају основне као и најновије научне радове који су у вези са темом дисертације, а који су објављени у међународним часописима (40) и зборницима радова међународних конференција (88) што потврђује значај, релевантност и савременост теме. Такође, међу референцама је наведен и рад који је кандидат објавио као аутор верификујући доприносе дисертације.

3.3. Опис и адекватност примењених научних метода

У овој дисертацији је коришћен мултидисциплинарни методолошки приступ у различитим фазама рада. Тиме је осигурана поузданост и валидност добијених резултата. Најпре је извршена систематична критичка анализа научне литературе у области заштите приватности на интернету и посебно на мрежном слоју, ради сагледавања тренутног стања и идентификовања недостатака постојећих система. Затим је, применом формалних метода моделовања и пројектовања, развијен концепт и архитектура *LISPP* система, заснована на примени шифровања са очувањем формата. Практична валидација теоријских концепата остварена је кроз имплементацију *LISPP* система у хардверском и софтверском облику са различитим варијантама имплементације како би се проверио квалитет појединих нових мрежних концепата (попут језика P4). На крају, за оцену перформанси примењен је метод експерименталне евалуације у строго дефинисаним реалним и виртуелним тестним окружењима. Уз помоћ стандардизованих алата за мерење мрежних перформанси (*iPerf2*, *PF_RING Zero Copy*, *Sockperf*), извршено је прецизно мерење протока пакета, пропусног опсега и унетог кашњења. У последњем делу рада верификација концепта за заштиту приватности *DNS* упита је извршена у реалним условима, на интернету, уз коришћење продукционих сервера компаније *Cloudflare*, чиме је доказана и практична применљивост и супериорност у перформансама предложеног *LISPP* система. Такође, анализа статистичких особина временског низа броја *DNS* упита на основу логова продукционог сервера са респектабилним бројем упита осигурава да су добијени резултати анализе и изведен предлог стратегије промене кључева поуздани и применљиви у пракси. Оваква комбинација метода сматра се потпуно адекватном и оправданом, јер омогућава да се објективно потврде све постављене хипотезе.

3.4. Применљивост остварених резултата

Имајући у виду да заштита приватности уопште, а посебно на мрежном слоју, представља озбиљан актуелни проблем, недвосмислено се отвара широк простор за практичну примену предложеног *LISPP* система. Коришћење шифровања са очувањем формата омогућава фину грануларност приликом анонимизације одабраних поља заглавља пакета која идентификују корисника. Овим пионирским приступом је у потпуности елиминисана потреба за изменом стандардног формата заглавља пакета, као и за комплексним одржавањем стања сесија током рада, што *LISPP* систем чини изузетно практичним и применљивим.

Интеграција *LISPP* система у постојећу интернет инфраструктуру директно је изводљива и не захтева никакве њене претходне модификације. Овај процес је додатно поједностављен и учињен економски прихватљивим захваљујући флексибилности технологија коришћених зарад имплементације. Истовремено, кроз свеобухватну експерименталну евалуацију доказано је да су перформансе *LISPP* система задржане на високом нивоу и да омогућавају заштиту комплетног саобраћаја малих и средњих мрежа са релативно јефтиним наменским програмабилним мрежним картицама.

Применљивост остварених резултата додатно је потврђена на конкретном примеру заштите приватности у домену *DNS* сервиса која је изведена у реалним условима коришћењем

продукционих сервера на интернету. У ту сврху, извршена је анализа лог датотека једног од *DNS* сервера Академске мреже Србије, намењеног обради упита корисника из основних и средњих школа. Установљено је да мрежни саобраћај забележен у посматраном *DNS* логу може бити заштићен без икаквих потешкоћа у погледу његовог обима. Штавише, утврђено је да би *LISPP* систем могао ефикасно да опслужи и заштити саобраћај чији је обим већи за чак три реда величине.

3.5. Оцена достигнутих способности кандидата за самостални научни рад

Током докторских студија кандидат је детаљно истражио и прегледао литературу из области заштите приватности на мрежном слоју, те је показао да је способан да сагледа тренутно стање области, предности и недостатке постојећих решења. Током истраживања теме дисертације кандидат је успео да постави хипотезе истраживања и да их на ваљан начин провери и верификује, што је резултирало објављивањем научног рада кандидата у истакнутом међународном часопису. Кандидат је током израде дисертације предложио ново решење које превазилази проблеме свих постојећих решења, а потом дато решење успешно имплементирао и експериментално евалуирао како би биле тестиране и верификоване полазне хипотезе. На основу свега наведеног, можемо закључити да је кандидат Марко Мићовић показао задовољавајући степен способности за самостални научни рад.

4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

4.1. Приказ остварених научних доприноса

Главни доприноси дисертације су остварени у следећим правцима:

- Преглед и свеобухватна анализа постојећих решења за заштиту од профилисања коришћењем података добијених анализом мрежног саобраћаја који обухвата начине њиховог функционисања као и сажетак познатих недостатака сваког од датих решења.
- Доказ оправданости коришћења алгоритама шифровања са очувањем формата у сврху замагљивања поља заглавља пакета.
- Предложена је оригинална методологија за заштиту приватности на мрежном слоју са следећим особинама уз коришћење шифровања са очувањем формата. Методологија је имплементирана као систем који је: транспарентан за корисника, без чувања стања приликом рада, независност од конкретног протокола, једноставна конфигурација, усклађеност са правним прописима. Ово су јединствене особине које други научни резултати до сада нису показали у овој области.
- Имплементација предложеног *LISPP* система за заштиту приватности за наменски хардвер на програмабилним мрежним картицама у више варијанти имплементација као и за *eBPF* технологију.
- Резиме ограничења процеса имплементације у случају конфигурисања равни података мрежних картица коришћењем *P4* језика.
- Анализа механизма за детекцију оптималног тренутка за промену коришћеног криптографског материјала у циљу несметаног рада и очувања постојећих токова података.
- Евалуација примене предложеног *LISPP* система за заштиту приватности у поставци са истим циљем као и „несвесни” *DNS* преко *HTTPS*, али са бољим перформансама.

4.2. Критичка анализа резултата истраживања

На основу увида у полазне хипотезе, циљ истраживања и остварене резултате, може се закључити да је успешно одговорено на сва релевантна истраживачка питања ове дисертације. Првобитно је извршена детаљна анализа постојећих механизма за заштиту приватности на мрежном слоју којом је недвосмислено констатован проблем употребе класичних блоковских алгоритама шифровања. Стога је, као директан одговор на уочена ограничења, предложена иновативна употреба шифровања са очувањем формата у циљу замагљивања поља заглавља пакета помоћу којих је могуће идентификовати корисника. На тим темељима је пројектован *LISPP* систем са могућношћу потпуно транспарентног замагљивања поља заглавља пакета без измене изворног формата пакета. Оваквим приступом је остварена висока ефикасност заштите приватности на мрежном слоју уз релаксиране гаранције, при чему је у потпуности елиминисана потреба за комплексним чувањем стања активних сесија током рада система.

Теоријски концепт је успешно преточен у праксу кроз више различитих имплементација, при чему је хардверска реализација извршена на програмабилним мрежним картицама, док је софтверска алтернатива остварена унутар језгра Линукс оперативног система применом *eBPF* технологије. Свеобухватна експериментална евалуација ових решења је спроведена у стварним и виртуелним окружењима, респективно, коришћењем релевантних алата за надгледање мреже. Резултати ових тестирања потврђују да је могуће остварити проток великог броја пакета и задржавање минималног и конзистентног кашњења. Додатно, као практичан случај употребе, предложен је *LDoH* сервис за анонимизацију *DNS* саобраћаја кроз замагљивање *IP* адреса клијената, чиме је избегнуто ослањање на вишеструко шифровање. Коначно, евалуацијом *LDoH* сервиса је доказано да су његове перформансе и до 45% боље у поређењу са алтернативним *ODoH* системом, чиме је потврђен значај предложеног решења.

4.3. Верификација научних доприноса

Кандидат Марко Мићовић је објавио следећи рад који је у непосредној вези са дисертацијом:

Категорија M22:

1. M. Mićović, U. Radenković, P. Vuletić, Network Layer Privacy Protection Using Format-Preserving Encryption, Electronics , Vol. 12, No. 23, pp. 1 – 21, Nov, 2023. [ISSN: 2079-9292, M22, IF₂₀₂₂=2.9, doi: [10.3390/electronics12234800](https://doi.org/10.3390/electronics12234800)]

5. ЗАКЉУЧАК И ПРЕДЛОГ

Дисертација под насловом „Заштита приватности на мрежном слоју применом шифровања са очувањем формата” кандидата Марка Мићовића представља значајан научни допринос у области рачунарске технике и информатике, а посебно у областима заштите приватности на интернету, мрежне безбедности и програмабилних мрежних уређаја и софтверских компоненти. Значај рада лежи у оригиналном приступу који омогућава ефикасно сакривање *IP* адреса корисника интернета уз минимално додатно кашњење, могућност рада без чувања стања конекција на мрежним уређајима, транспарентност рада за обе актуелне верзије *IP* протокола и очување формата пакета.

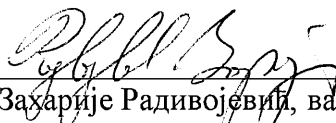
У оквиру рада кандидат је изложио свеобухватну анализу изазова заштите приватности на мрежном слоју, прецизно указујући на недостатке постојећих механизма изазваних услед ослањања на класично блоковско шифровање. Као одговор на уочене недостатке, пројектован је *LISPP* систем који примењује шифровање са очувањем формата. Практична изводљивост овог концепта је успешно доказана имплементацијом за програмабилне мрежне картице коришћењем *P4* и *Micro-C* језика, као и софтверском реализацијом унутар језгра Линукс оперативног система применом *eBPF* технологије. Спроведена експериментална евалуација у реалним условима потврђује да систем уноси минимална кашњења, чиме се

предложено решење позиционира као потпуно адекватно за обраду мрежног саобраћаја великог протока пакета. На основу анализе реалних мрежних оптерећења, установљено је да пројектовани *LISPP* систем може бити једноставан, економичан и тренутно интегрисан у постојећу интернет инфраструктуру без њених претходних модификација. Свеукупно гледано, ова дисертација дефинише потпуно нови правац за ефикасну заштиту приватности корисника на мрежном слоју. Дисертација јасно илуструје потенцијал шифровања са очувањем формата у контексту заштите приватности на мрежном слоју, а резултати изложени у дисертацији су верификовани објављеним научним радом кандидата. Кандидат је спроведеним истраживањем показао способност за даљи самостални научно-истраживачки рад.

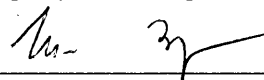
На основу свега наведеног, Комисија констатује да је кандидат Марко Мићовић испунио све формалне и суштинске услове предвиђене Законом о високом образовању, Статутом и Правилником о докторским студијама Електротехничког факултета Универзитета у Београду. Комисија има задовољство да предложи Наставном-научном већу Електротехничког факултета Универзитета у Београду да се докторска дисертација под насловом „Заштита приватности на мрежном слоју применом шифровања са очувањем формата” кандидата Марка Мићовића прихвати, изложи на јавни увид и упути на коначно усвајање Већу научних области техничких наука Универзитета у Београду.

У Београду, 01.04.2026.

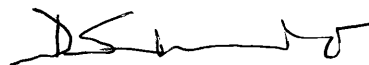
ЧЛАНОВИ КОМИСИЈЕ



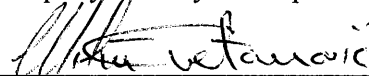
др Захарије Радивојевић, ванредни професор
Универзитет у Београду – Електротехнички факултет



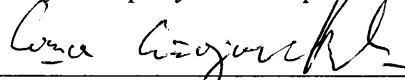
др Зоран Чича, редовни професор
Универзитет у Београду – Електротехнички факултет



др Дејан Симић, редовни професор
Универзитет у Београду – Факултет организационих наука



др Милош Цветановић, ванредни професор
Универзитет у Београду – Електротехнички факултет



др Саша Стојановић, ванредни професор
Универзитет у Београду – Електротехнички факултет