

|                      |      |        |          |
|----------------------|------|--------|----------|
| ПРИМЉЕНО: 04 02 2025 |      |        |          |
| Орг. јед.            | Број | Прилог | Вредност |
|                      | 233  |        |          |

НАСТАВНО-НАУЧНОМ ВЕЋУ

**Предмет:** Оцена научне заснованости теме докторске дисертације кандидаткиње Јелице Радомировић.

Одлуком 2040/27 бр. Од 5.11.2024. године, именовани смо за чланове Комисије за оцену научне заснованости теме докторске дисертације кандидаткиње Јелице Радомировић за израду докторске дисертације и научне заснованости теме „Једна нова класа система за дестилацију апсолутно тајних криптографских кључева заснованих на заједничкој случајности“.

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

**ИЗВЕШТАЈ**

**1. Подаци о кандидату**

**1.1. Биографски подаци**

Јелица Радомировић је рођена 3.7.1997. године у Београду. Завршила је основну школу „Раде Кончар“ у Земуну као ђак генерације. Након основе школе уписује Математичку гимназију у Београду коју завршава са одличним успехом уз освајање награде на државном такмичењу из физике. Електротехнички факултет у Београду уписује 2016. године. Била је студент на катедри за Сигнале и системе, а дипломирала је у септембру 2020. године са просечном оценом 9,13. Дипломски рад под називом „Препознавање карактера знаковоног језика КНН методом“ под менторством проф. др Александре Крстић одбранила је у септембру 2020. године са оценом 10.

Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за сигнале и системе уписала је у октобру 2020. године а завршила у септембру 2021. године са просечном оценом 9,83. Мастер рад под називом „Фузија слика термалне камере и камере у видљивом делу спектра“ под менторством проф. др Вељка Папића одбранила је са оценом 10.

Докторске академске студије уписала је у октобру 2021. године на Електротехничком факултету у Београду на модулу Управљање системима и обрада сигнала. Област њеног истраживања обухвата обраду сигнала, теорију информација, криптографију и неуралне мреже. Резултат ових истраживања је пет објављених радова у међународним научним часописима (по један рад категорија M21a и M21, три рада категорије M22) и један рад на међународној конференцији.

Од августа 2021. запослена је у Влатаком институту високих технологија као истраживачко развојни инжењер. На тој позицији доминантно је радила на развоју

алгоритама за генерисање тајних кључева базираних на изворима заједничке случајности. Осим тога, у оквиру области машинског учења радила је и на моделовању високопрецизних предиктора из више различитих проблемских домена.

## 1.2. Стечено научноистраживачко искуство

Кандидаткиња је током докторских академских студија на Електротехничком факултету Универзитета у Београду (модул Управљање системима и обрада сигнала) активно учествовала у научним истраживањима која су резултовала полагањем следећих испита:

- Оптимални и адаптивни стохастички системи (Оцена 10, 9 ЕСПБ бодова)
- Технике обраде и препознавање говорног сигнала (Оцена 10, 9 ЕСПБ бодова)
- Класификација и естимација сигнала (Оцена 10, 9 ЕСПБ бодова)
- Сложени мулти-агент системи (Оцена 10, 9 ЕСПБ бодова)
- Одабране примене дигиталне обраде слике (Оцена 10, ЕСПБ бодова 9)
- Мултимедијални системи - одабрана поглавља (Оцена 10, 9 ЕСПБ бодова)
- Неуралне мреже (Оцена 10, 9 ЕСПБ бодова)

У оквиру студија завршене су и остале обавезе:

- Студијски истраживачки рад I (24 ЕСПБ бодова)
- Студијски истраживачки рад II (24 ЕСПБ бодова)

Поред испита, у току докторских студија кандидаткиња је обављала научноистраживачке активности у оквиру научне институције у којој је запослена, а које су, заједно са испитима, довеле до објављивања радова у међународним часописима и на конференцијама

Списак објављених радова:

Часописи:

1. Galis M., Milosavljević M., Jevremović A., Banjac Z., Makarov A., Radomirović J.: *Secret-Key Agreement by Asynchronous EEG over Authenticated Public Channels*, - Entropy, Vol 23, No 10, 2021, 1327.
2. Radomirović J., Milosavljević M., Kovačević B., Jovanović M.: *Privacy Amplification Strategies in Sequential Secret Key Distillation Protocols Based on Machine Learning*, - Symmetry, Vol 14, No 10, 2022, 2028.
3. Radomirović J., Milosavljević M., Banjac Z., Jovanović M.: *Secret Key Distillation with Speech Input and Deep Neural Network-Controlled Privacy Amplification*, - Mathematics, Vol 11, No 6, 2023, 1524.
4. Vesovic R., Milosavljevic M., Punt M., Radomirovic J., Bascarevic S., Savic M., Milenkovic V., Popovic M., Ercegovac M.: *The role of the diaphragm in prediction of respiratory function in the immediate postoperative period in lung cancer patients using a machine learning model*, - World Journal of Surgical Oncology, Vol 21, 2023, 393.
5. Vesovic R., Milosavljevic M., Punt M., Radomirovic J.: *A Machine Learning Multilayer Meta-Model for Prediction of Postoperative Lung Function in Lung Cancer Patients*, - Applied Sciences, Vol. 14, No. 4, 2024, 1566.

Конференције:

6. Radomirović, J., Milosavljevic, M., Krstić, A. *Secret Keys Distillation using Speech Signals and Discussion over Public Authenticated Channel*, - Proceedings of the 9th International

Наводи се списак објављених радова или других релевантних резултата и активности који доказују афинитет кандидата за рад на приложеној теми.

### 1.3. Оцена подобности кандидата за рад на предложеној теми

На основу претходног приказа резултата досадашњег научноистраживачког рада, може се констатовати да је кандидаткиња Јелица Радомировић усредсређена на истраживање актуелне теме у области криптографије које се односи на генерисање и дистрибуцију криптографских кључева, као и да поседује истраживачко искуство које је квалификује за израду предложене теме.

Досадашњи научни доприноси кандидаткиње верификовани су кроз више научних радова у међународним часописима и на конференцијама.

Кандидат је у току презентације теме детаљно образложио предмет и циљ докторске дисертације, полазне хипотезе истраживања, планиране методе истраживања, као и очекиване научне доприносе. У својим одговорима на сва постављена питања од стране чланова Комисије, дао је задовољавајуће одговоре и образложења.

Стога, Комисија препоручује да се кандидату Јелица Радомировић, мастер инжењеру електротехнике и рачунарства одобри израда предложене докторске тезе под називом „Једна нова класа система за дестилацију апсолутно тајних криптографских кључева заснованих на заједничкој случајности“.

## **2. Предмет и циљ истраживања**

Једна од основних компоненти сваког криптографског система су тајни кључеви, који претходно морају бити размењени између легитимних учесника заштићене комуникације. Процес синтезе и дистрибуције тајних кључева један је од примарних проблема разматраних у домену криптографске теорије и праксе. Ова проблематика актуелизована је развојем бежичних комуникација, интернета и посебно интернета ствари (*Internet of Things - IoT*), као и рањивости ове инфраструктуре у готово свим сценаријима савремених сајбер напада. Ако имамо у виду основни Шенонов резултат [1] да апсолутна тајност преношених порука захтева тајне кључеве дужине не мање од порука, може се рећи да су извори случајности постали стратешки ресурс у истој равни са традиционалним ресурсима као што су енергенти и друга природна богатства. У техничком смислу то значи да сваки извор случајности, идентификован унутар савремене рачунарско комуникационе инфраструктуре, потенцијално омогућава генерисање довољне количине тајних кључева за потребе апсолутно тајног комуницирања. Стога, актуелност сајбер безбедности потенцира важност развоја области генерисања и дистрибуције тајних криптографских кључева. Тренутна решења подразумевају директну дистрибуцију кључева између два легитимна учесника сигурним каналима, коришћење приватног и јавног кључа у јавно доступним алгоритмима, класичну физичку дистрибуцију, путем посредника и друга мање ефикасна решења. Проблеми на које се наилази у овим решењима су потреба за обезбеђивањем сигурних канала, временска комплексност која ограничава комуникацију у реалном времену, немогућност реализације дистрибуције у одређеним ситуацијама као и све извеснија појава квантних рачунара која ће довести до повећања рачунарских ресурса противника. Све наведено отвара могућности развоја једне нове класе система која би превазишла описане проблеме а уједно искористила потенцијал извора заједничке случајности.

Темељи новог приступа за генерисање криптографских кључева постављени су у радовима *Ahlsved-a* и *Csiszar-a* [2], *Maurer-a* [3] и *Csiszar-a* и *Naraian-a* [4] где је представљена идеја о екстракцији криптографских кључева из међусобно корелисаних сигнала довољно

великих ентропија. Теоријски посматрано, реч је о дискретном извору без меморије (*Discrete Memoryless Source - DMS*), чије су корелисане реализације доступне учесницима протокола. Уколико је могуће екстраховати тајне кључеве брзином већом од нуле, каже се да дати *DMS* поседује заједничку случајност (*Common Randomness - CR*) позитивног капацитета. У односу на локацију извора неодређености, разликују се два приступа екстракције сигнала, [3]: из *DMS*-а независних од комуникационих канала, такозвани модел извора (*source model*) и из *DMS*-а кога представља сам коришћени комуникациони канал, такозвани модел канала (*channel model*). Maurer-ов секвенцијални протокол дестилације кључева на основу јавне дискусије (*Sequential Key Distillation by public discussion - SKD*) [3] најпознатији је протокол за сигурну размену кључева. Његов циљ је усклађивање информација легитимних учесника протокола, што резултује заједничким кључем о коме нападач на систем нема никакве информације.

Легитимни учесници у оквиру протокола размењују поруке преко двосмерног јавног аутентификованог канала без грешака (тзв. јавна дискусија), док је потенцијалним нападачима на систем доступан јавни канал и све поруке које су по њему размењене. *SKD* протокол обухвата 4 фазе дестилације кључа [3], дељење случајности, дестилација предности (*advantage distillation - AD*), усклађивање информација (*information reconciliation - IR*) и појачавање приватности (*privacy amplification - PA*).

У предложеној докторској дисертацији биће разматран искључиво модел извора као *CR* и одговарајући *SKD* протокол са јавном дискусијом. Овакав избор има више предности, првенствено у професионалним и војним применама у којима се поштује принцип минимизације ризика компромитовања целог система ако је компромитован један његов подсистем. Према том принципу, *SKD* систем треба да буде независан од других криптографских и телекомуникационих модула. Ова чињеница искључује могућност коришћења *SKD*-а заснованог на моделу канала, а фаворизује *SKD* заснован на моделу извора.

Циљ ове докторске дисертације је детаљнија теоријска анализа и практична евалуација *PA* блока. Као што је познато, његова примарна намена је минимизација количине информација коју добија нападач у току праћења извођења *SKD* протокола са јавном дискусијом. Уколико је *PA* блок базиран на хеш функцијама, нападачева условна *Renyi* ентропија другог реда, (*Evesdropper Conditional Renyi Entropy of order 2 - ECRE2*), теоријски одређује максималну дужину тајног кључа тако да нема цурења информација ка нападачу [5]. Уобичајена ствар која се ради у пракси базирана је на утврђивању глобалне доње границе за *ECRE2* за дати извор. Ова константа се затим користи за одређивање излазне димензије универзалне класе хеш функција за све појединачне реализације протокола. Овим поступком је оптимална стратегија базирана на локално одређеној доњој граници *ECRE2* замењена далеко лошијом усредњеном глобалном границом. Последице примене глобалне доње границе су добијање значајно краћих тајних кључева на излазу *PA* блока и непоуздана процена цурења информација ка нападачу. Друга уобичајена ствар у пракси базирана је на (углавно погрешној) претпоставци да су улазне секвенце у *PA* блок некорелисане са одговарајућим опсервацијама нападача. *PA* блок је тада дизајниран тако да елиминише искључиво оне информације које су добијене опсервирањем комуникације преко јавног канала. Последице оваквог приступа су одсуство мере за процену количине процуреле информације јер се она елимише, непоуздана процена сигурносне маргине за генерисање тајних кључева и потреба испитивања исправности коначних секвенци проласком кроз неки стандардни пакет статистичких тестова. Да бисмо превазишли поменуте недостатке које се примењују у пракси у овој дисертацији предлаже се нова методологија појачања приватности базирана на машинском учењу која естимира *ECRE2* и његову доњу границу. За естиматор *ECRE2* се предлаже дубока неуронска мрежа за предикцију интервала (*Prediction Interval Deep Neural Network block - PIDNN*). Улаз у *PIDNN* су обележја локално измерена на страни легитимних учесника, док се обучавање врши у офлајн режиму на скуповима примера генерисаним задатим извором заједничке случајности. Посебна пажња ће бити посвећена

избору најинформативнијих обележја, укључујући и трансформацију улазних низова у форму погоднију за примену технологија за обраду природних језика (*Natural Language Processing Technologies - NLP*). Ова докторска дисертација такође има циљ идентификацију и експерименталну евалуацију нових извора заједничке случајности, погодних за практичну употребу. Предлаже се детаљнија анализа биометријских сигнала, конкретно електроенцефалографских (ЕЕГ) и говорних сигнала који се показују као погодан извор за *SKD* протокол са јавном дискусијом. Потенцијал ових биометријских сигнала као извора заједничке случајности није идентификован и истраживан у доступној литератури.

#### Референце:

1. Shannon, C.E. Communication Theory of Secrecy Systems\*. Bell Syst. Tech. J. 1949, 28, 656–715, <https://doi.org/10.1002/j.1538-7305.1949.tb00928.x>.
2. Ahlswede, R.; Csiszar, I. Common randomness in information theory and cryptography. Part I: Secret sharing. IEEE Trans. Inf. Theory 1993, 39, 1121–1132.
3. Maurer, U.M. Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory 1993, 39, 733–742.
4. Csiszar, I.; Narayan, P. Secrecy Capacities for Multiple Terminals. IEEE Trans. Inf. Theory 2004, 50, 3047–3061.

Bennett, C.H.; Brassard, G.; Crepeau, C.; Maurer, U.M. Generalized privacy amplification. IEEE Trans. Inf. Theory 1995, 41, 1915–1923. <https://doi.org/10.1109/18.476316>.

### 3. Полазне хипотезе

Полазне хипотезе докторске дисертације кандидаткиње су:

- Ефикасност *SKD* протокола може се значајно унапредити применом нових *PA* стратегија заснованих на процени локалних вредности *ECRE2*.
- Дубоке неуронске мреже за предикцију интервала, потенцијално могу бити ефикасни предиктори локалних вредности *ECRE2*.
- Подскупови најинформативнијих обележја на улазу у предикциони блок, могу се добити на основу трансформације изворних секвенци извора заједничке случајности у облик који је погодан за издвајање стилометријских обележја уобичајених у области обраде природних језика.
- Биометријски сигнали могу бити ефикасни извори заједничке случајности, погодни за дизајнирање практичних *SKD* система високих перформанси.

### 4. Научне методе истраживања

Предложена докторска дисертација захтева теоријско експериментални истраживачки поступак. У оквиру теоријских истраживања неопходно је применити методе уобичајене у домену теорије информација и кодовања, стохастичких система и анализе сигнала. Гарантоване перформансе *SKD* система захтевају теоријску анализу информационих токова цурења информација ка нападачу, које се базирају на мање познатим информационим мерама, као што су *Renyi*-јева ентропија, условна *Renyi*-јева ентропија и различите Шенонове ентропије вишег реда. Дизајнирање *PA* блока на основу *PIDNN*, захтева примену метода синтезе система машинског учења и избора најинформативнијих обележја из домена *NLP*-а. Анализа конвергентних својстава сложених алгоритама машинског учења захтева примену метода развијених у оквиру стохастичких система, теорије вероватноће и статистике. Будући да су критеријуми обучавања *PIDNN* регуларизационог типа, неопходно је познавање и адекватна примена регуларизационе теорије из домена нелинеарне оптимизације.

Експериментални поступак примењен у овој докторској дисертацији обухвата не само евалуацију синтетисаних *SKD* система, већ и адекватан одабир репрезентативних сигнала за ове потребе. Будући да ће се експерименти доминантно обављати на биометријским изворима заједничке случајности, неопходно је применити адекватан методолошки оквир за одабир субјеката давалаца ових сигнала уз поштовање свих прописаних етичких норми.

## **5. Очекивани научни допринос**

Очекивани научни доприноси које је кандидат образложио су:

1. Синтеза нове класе система за генерисање криптографских кључева високог квалитета базираних на протоколима секвенцијалне дестилације и јавне дискусије.
2. Синтеза ефикасних *PA* стратегија заснованих на процени локалних вредности *ECRE2*.
3. Налажење најинформативнијих подскупова локално мерљивих обележја за потребе обучавања *PIDNN*.
4. Формулисање нових квантитативних показатеља степена искоришћења задатог извора заједничке случајности.
5. Евалуација ефикасности ЕЕГ и говорног сигнала као извора заједничке случајности.

## **6. План истраживања и структура рада**

План истраживања који је кандидат изложио је следећи:

1. Ревизија литературе о постојећим методама синтезе и дистрибуције тајних кључева.
2. Анализа и компарација различитих извора заједничке случајности.
3. Дизајн система, са новим стратегијама рада *PA* блока, заснованим на процени локалних вредности *ECRE2*.
4. Експериментална евалуација перформанси предложеног система на биометријским изворима заједничке случајности, посебно ЕЕГ и говорног сигнала.

## **7. Закључак и предлог**

На основу приложене документације и увида у досадашњи рад кандидаткиње Јелице Радомировић, Комисија оцењује да кандидаткиња располаже потребним знањем и вештинама неопходним за адекватно разумевање и истраживање предложене теме. На основу објављених научних радова, детаљног образложења теме докторске дисертације и успешне јавне одбране, закључује се да је кандидат способан за самостални научно-истраживачки рад, да може да изврши планирана истраживања у целости, као и да испуњава све формалне и суштинске услове да приступи изради докторске дисертације.

Предложена тема се бави новим приступом у генерисању и дистрибуцији криптографских кључева. Предмет и циљ дисертације јасно су формулисани, а у складу са њима су постављене хипотезе и план истраживања. Имајући у виду значај, актуелности и брзину напретка технологије који изискују нове и софистициране методе заштите, Комисија констатује да предложена тема представља значајно и атрактивно научно-истраживачко подручје. Резултати теме ће представљати значајан и оригинални научни допринос, који могу бити од велике користи за имплементацију у већ постојећим као и новим системима заштите.

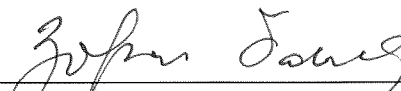
Комисија предлаже за ментора др Бранка Ковачевића, професора емеритуса Универзитета у Београду – Електротехнички факултет.

На основу претходно изложеног, Комисија сматра да су кандидаткиња и предложена тема подобни, те са задовољством предлаже Наставно-научном већу Електротехничког факултета Универзитета у Београду да кандидаткињи Јелици Радомировић, мастер инжењерки електротехнике и рачунарства, одобри израду докторске дисертације под називом „Једна нова класа система за дестилацију апсолутно тајних криптографских кључева заснованих на заједничкој случајности“. Предложена тема припада акредитованом студијском програму Електротехника и рачунарство, односно научној области Управљање системима и обрада сигнала, на Електротехничком факултету Универзитета у Београду.

#### ЧЛАНОВИ КОМИСИЈЕ



др Горан Квашчев, редовни професор  
Универзитет у Београду – Електротехнички факултет



др Зоран Бањац, виши научни сарадник  
Институт Влатаком, Београд



др Павле Вулетић, ванредни професор  
Универзитет у Београду – Електротехнички факултет