

Beograd
Danijelova 32

Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj 4-71/2025 od 10.04.2025.godine, određeni smo za članove Komisije za pregled, ocenu i usmenu odbranu doktorske disertacije Dejana Cizelja, pod nazivom: *"Sinteza efikasnih izvora zajedničke slučajnosti za potrebe generisanja i distribuciju tajnih kriptografskih ključeva"*.

Posle pregleda dostavljene disertacije i drugih pratećih materijala, Komisija je sačinila sledeći

REFERAT

1. UVOD

1.1. Hronologija odobravanja i izrade disertacije

Dejan Cizelj je upisao doktorske studije na Singidunum univerzitetu školske 2022/2023. godine. Položio je sve ispite predviđene planom doktorskih studija. Zahtev za odobravanje teme za izradu doktorske disertacije podneo je 26.02.2025. godine. Odlukom Veća Departmana za poslediplomske studije Univerziteta Singidunum, broj 4-37/2025 od 06.03.2022. godine, formirana je Komisija u sastavu:

1. Prof. dr Miljan Vučetić, redovni profesor, Univerzitet Singidunum, Beograd
2. Prof. dr Mladen Veinović, redovni profesor, Univerzitet Singidunum, Beograd
3. Dr Tomislav Unkašević, naučni saradnik, Institut Vlatacom, Beograd
4. Dr Branko Kovačević, profesor emeritus Elektrotehnički fakultet, Univerzitet Beograd

za ocenu teme i podobnosti kandidata za izradu doktorske disertacije pod nazivom: *"Sinteza efikasnih izvora zajedničke slučajnosti za potrebe generisanja i distribuciju tajnih kriptografskih ključeva"*. Na osnovu pozitivnog izveštaja Komisije Veće Departmana za poslediplomske studije Univerziteta Singidunum je 10.04.2025. godine odobrilo rad na izradi doktorske disertacije i donelo odluku o obrazovanju Komisije za ocenu i odbranu doktorske disertacije pod naslovom: *"Sinteza efikasnih izvora zajedničke slučajnosti za potrebe generisanja i distribuciju tajnih kriptografskih ključeva"*, kandidata Dejana Cizelja, mastera računarstva i informatike, u sastavu:

1. Prof. dr Miljan Vučetić, redovni profesor, Univerzitet Singidunum, Beograd
2. Prof. dr Mladen Veinović, redovni profesor, Univerzitet Singidunum, Beograd
3. Dr Tomislav Unkašević, naučni saradnik, Institut Vlatacom, Beograd
4. Dr Branko Kovačević, profesor emeritus Elektrotehnički fakultet, Univerzitet Beograd

1.2. Naučna oblast disertacije

Tema disertacije kandidata je u oblasti računarstva i informatike za koju je Univerziteta Singidunum matičan.

1.3. Biografski podaci kandidata

Dejan Cizelj, rođen 5. aprila 1980. u Beogradu, poseduje državljanstvo Srbije i Izraela. Svoje obrazovanje stekao je u Izraelu i Bosni i Hercegovini. Na Lauder School of Government pri Interdisciplinary Center Herzliya (danas Reichman University) završio je osnovne i master studije iz oblasti državne uprave, sa fokusom na međunarodne odnose, bezbednost, borbu protiv terorizma i sajber bezbednost. Takođe, poseduje master diplomu iz računarstva i informatike Univerziteta Sinergija u Bijeljini.

Profesionalno, Dejan ima bogato iskustvo u informacionoj bezbednosti. Trenutno je angažovan u izraelskoj fintech startup kompaniji Papaya Global, gde upravlja informacionom sigurnošću. Njegove odgovornosti uključuju razvoj i implementaciju bezbednosnih politika i procedura, identifikaciju i rešavanje bezbednosnih pretnji, kao i istraživanje incidenata. Posebnu pažnju posvećuje usklađivanju sa međunarodnim standardima kao što su HIPAA, HITRUST, NIST, ISO 27001 i 22301.

Pre ove pozicije, radio je na istoj poziciji u zdravstvenoj startup kompaniji Healthi.io, i takođe kao viši menadžer za bezbednost informacija i usklađenost u kompaniji Ernst & Young Israel. Tamo je vodio tim koji je sprovodio IT revizije, bezbednosne procene, izveštavanje i primenu standarda kao što su SOC 1, SOC 2+, ITGC i ISO 27001.

Dejan je ranije bio i menadžer razvoja poslovanja u firmi specijalizovanoj za unutrašnju bezbednost, gde je stekao iskustvo u analizi tržišta i izgradnji strateških partnerstava u sektoru odbrane i bezbednosti. Njegova stručnost i karijerni put svedoče o snažnoj posvećenosti informacionoj bezbednosti, kojoj se intenzivno posvetio nakon završenih studija u Izraelu.

2. OPIS DISERTACIJE

2.1. Sadržaj disertacije

Doktorska disertacija pod naslovom: „*Sinteza efikasnih izvora zajedničke slučajnosti za potrebe generisanja i distribuciju tajnih kriptografskih ključeva*“ ima ukupno 104 strane. Disertacija ima 8 poglavlja i spisak literature. Poglavlja su:

1. Uvod
2. Osnove teorije kriptografskih ključeva
3. Pregled relevantne literature i modela izvora zajedničke slučajnosti
4. Arhitektura novog perfektno tajnog kripto sistema
5. Informaciono-teorijska analiza izvora zajedničke slučajnosti
6. Optimalni SKD sistem zasnovan na CR KSG i WINNOWER IR protokolu
7. Analiza bezbednosti i praktični aspekti primene
8. Zaključak i pravci budućih istraživanja
9. Literatura

U disertaciji ima ukupno 20 slika i 4 tabele. Literatura sadrži 39 bibliografskih jedinica.

2.2. Kratak prikaz pojedinačnih poglavlja

Nakon uvodnog dela, u kome su predstavljeni osnovni pojmovi, istraživački okvir i ciljevi rada, disertacija se dalje razvija kroz osam poglavlja, strukturiranih tako da prate logički tok razvoja predložene metodologije i sistema.

Poglavljje 2 donosi teorijske osnove vezane za generisanje i upotrebu kriptografskih ključeva u kriptografskim sistemima. Poseban akcenat stavljen je na definisanje ključnih osobina koje tajni ključevi moraju da poseduju kako bi se obezbedila kriptografska sigurnost, uključujući nepredvidivost, entropiju i njen nivo.

Poglavljje 3 sadrži pregled relevantne naučne i stručne literature, sa fokusom na postojeće modele zajedničke slučajnosti (IZS) koji se koriste za sintezu sigurnosnih ključeva. Analiziraju se koncepti i pristupi koji su prethodili ovom radu, pri čemu se identifikuju nedostaci postojećih rešenja i motiviše razvoj predloženog modela.

Poglavljje 4 posvećeno je detaljnom opisu predložene arhitekture sistema, koji funkcioniše kao autonomni i perfektno tajni sistem za generisanje binarnih sekvenci sa unapred zadatim korelacionim svojstvima neophodnim za izvore zajedničke slučajnosti. Ovako koncipiran sistem omogućava generisanje i distribuciju tajnih ključeva u realnom vremenu, nezavisan od kanala prenosa i kriptografskih algoritama koji se primenjuju za zaštitu primarnog izvora informacija.

Poglavljje 5 se bavi informaciono-teorijskom analizom predloženog izvora zajedničke slučajnosti. U ovom delu se izvode fundamentalne granice vezane za ekvivokaciju i sigurnost sistema, kao i optimalni dizajn koji se postiže implementacijom protokola za informacionu rekonstrukciju (IR), konkretno zasnovanog na Winnow-ovoj metodi.

Poglavljje 6 detaljno razmatra realizaciju sistema za generisanje tajnih ključeva (SKD) koji se oslanja na koncepciju determinističkog generatora CR-KSG (Common Randomness Key Stream Generator) i pomenutog WINNOW-IR protokol. Opisani su algoritamski koraci, struktura generatora, kao i njegov doprinos sigurnosnim performansama sistema.

Poglavljje 7 razmatra aspekte sigurnosti i implementacije predloženog sistema. Posebna pažnja posvećena je praktičnim izazovima, kompromisima u dizajnu i uticaju različitih parametara na performanse, kao i otpornosti sistema na različite vrste napada i neidealnosti u komunikacionom okruženju.

Poglavljje 8 obuhvata zaključna razmatranja u kojima se sumiraju glavni rezultati istraživanja, identifikuju ključni doprinosi disertacije i ukazuju potencijalni pravci za dalje unapređenje sistema i proširenje teorijskog modela u budućim radovima.

Poglavljje 9 predstavlja pregled direktno korišćene literature, obuhvatajući relevantne izvore koji su poslužili kao teorijska i metodološka osnova za sprovedeno istraživanje.

3. OCENA DISERTACIJE

3.1. Savremenost i originalnost

Predmet istraživanja ove doktorske disertacije je razvoj konceptualno novog i praktično primenljivog modela za sintezu izvora zajedničke slučajnosti (IZS), koji zadovoljava rigorozne zahteve bezbednosne, teorijske i komunikacione efikasnosti. U okviru predloženog pristupa, fokus je na oblikovanju IZS koji omogućava pouzdano generisanje i distribuciju tajnih ključeva između dve legitimne strane – uobičajeno označene kao Alisa i Bob – čak i u prisustvu aktivnog i informisanog protivnika Eve.

Model IZS koji je centralna tema ovog rada, projektovan je tako da ispunjava sledeće ključne kriterijume:

- Opšta dostupnost i simetrija posmatranja - sistem mora omogućiti da obe legitimne strane, koristeći dostupne ulazne podatke, mogu lokalno rekonstruisati identične sekvence zajedničke slučajnosti sa visokim stepenom pouzdanosti i niskim nivoom neslaganja.
- Integritet izvora - potencijalni protivnik (Eva) ne sme imati mogućnost da utiče na parametre izvora, niti da manipuliše njegovim ponašanjem tokom rada, čime se garantuje autonomnost procesa sinteze IZS.
- Informaciono-teorijska optimalnost - parametri konstrukcije izvora i pripadajućih protokola oblikovani su tako da maksimiziraju kapacitet tajnosti – tj. stopu kojom se može destilovati bezbedan ključ – u skladu sa teorijskim ograničenjima.
- Bezbednosna robusnost protokola - predloženi sistem mora obezbediti garantovanu donju granicu za stopu generisanja ključeva, kao i kontrolisanu gornju granicu za stopu curenja informacija prema protivniku. Ove garancije važe čak i pod pretpostavkom da Eva primenjuje optimalnu strategiju zaključivanja baziranu na potpunoj analizi svih javno dostupnih informacija i potpunom poznavanju arhitekture sistema.

U osnovi ovog modela nalazi se generator ključeva za šifrovanje (Key Stream Generator) zasnovan na zajedničkom tajnom ključu – KSG(K). U situacijama kada se izlazne sekvence ovog generatora lokalno „zašume“ ili poremete pomoću dodatnih nezavisnih izvora čiste slučajnosti, ponašanje rezultujućeg IZS približava se tzv. Mauerovom satelitskom modelu, koji je referentni okvir u oblasti sekvencijalne destilacije tajnih ključeva na osnovu javne diskusije. Ključna prednost ovakve konstrukcije je to što se svi relevantni parametri sistema – uključujući sintezu, distribuciju i destilaciju ključeva – mogu matematički precizno izraziti i analizirati u zatvorenoj formi, što omogućava teorijski strogu evaluaciju bezbednosti.

S druge strane, najosetljivija tačka ovog sistema leži u inicijalnom zajedničkom tajnom ključu K. Napadi na K predstavljaju potencijalnu pretnju celokupnoj bezbednosti sistema. Da bi se ocenila otpornost na takve napade, uvedena je Šenonova mera ekvivokacije, koja kvantifikuje neizvesnost ključa iz ugla napadača. U okviru ovog istraživanja konstruiše se klasa IZS kod kojih se može matematički utvrditi donja granica ekvivokacije, što direktno omogućava održivu i garantovanu sigurnu destilaciju ključeva u različitim operativnim režimima.

Istorijski gledano, koncept destilovanja tajnih ključeva iz korelisanih izvora je prvi formalizovao Ueli Maurer, koristeći metaforu satelitske komunikacije kako bi se ilustrovala mogućnost bezbedne ekstrakcije tajnosti u prisustvu treće strane koja prisluškuje. Njegov rad otvorio je široko polje istraživanja koje je našlo primenu u kvantnoj distribuciji ključeva (QKD), kao i u sistemima bezbednosti na fizičkom sloju u klasičnim komunikacionim kanalima.

Razvijeni protokoli kao što su Cascade i Winnow omogućavaju usklađivanje lokalno generisanih sekvenci između Alise i Boba uz minimalno curenje informacija kroz javni kanal. Ovi protokoli su znatno optimizovani za rad u uslovima visokog nivoa šuma ili ograničene propusnosti, što ih čini pogodnim za realne implementacije.

Bezbednosne analize zasnovane na meri ekvivokacije, inspirisane Šenonovim pionirskim radovima, postaju sve prisutnije u savremenim pristupima modelovanju sigurnosti. Ipak, većina postojećih sistema ne poseduje robustan mehanizam za održavanje konstantnog nivoa ekvivokacije u vremenu, što ovu disertaciju čini naročito značajnom.

Iako je koncept sintetičkih IZS baziranih na pseudoslučajnim strukturama sporadično razmatran u literaturi, dosadašnji radovi retko uključuju formalne, analitičke procene entropijskih karakteristika takvih sistema, niti ih povezuju sa adaptivnim protokolima za sekvencijalnu destilaciju ključeva (SKD).

Ova disertacija daje doprinos upravo u toj oblasti – uvodeći teorijski utemeljen, analitički modelovan i praktično ostvariv sistem koji koristi kombinaciju zajedničkog ključa i lokalnog izvora čiste slučajnosti za izgradnju pouzdanog i sigurnog IZS.

U ovom kontekstu, kandidat je svoju originalnost potvrdio na korektan i uverljiv način objavljivanjem radova u međunarodnim naučnim časopisima (1 rad u vodećem međunarodnom časopisu kategorije M21a+), u domaćim naučnim časopisima (1 rad) i zbornicima domaćih naučnih konferencija (2 rada).

3.2. Osvrt na referentnu i korišćenu literaturu

U izradi disertacije korišćena je literatura iz svih relevantnih oblasti uključujući najnovije radove u vrhunskim međunarodnim naučnim časopisima, kao i sopstvene reference. Na osnovu tih referenci, originalni naučni rezultati do kojih je kandidat došao u disertaciji su stavljani u odgovarajući naučni kontekst.

3.3. Opis i adekvatnost primenjenih naučnih metoda

Kandidat je u toku naučnog i istraživačkog rada upotrebio različite metode kako bi bili zadovoljeni osnovni metodološki zahtevi – objektivnost, pouzdanost, opštost i sistematičnost.

U skladu sa izabranom problematikom, definisanim ciljevima istraživanja i postavljenim naučnim hipotezama radi definisanja naučnih i stručnih zaključaka i iznalaženja mogućih rešenja upotrebljena je teorijska analiza uz korišćenje rezultata istraživanja iz međunarodne naučne literature, odnosno saznanja naučnika i drugih autora koji su istraživali problematiku kojom se bavi i ovaj rad. U disertaciji se predstavljaju naučno-teorijska saznanja, relevantna literatura i originalni predlozi

korišćenjem većeg broja metoda, i to: istorijske metode, metode kompleksnog posmatranja i analize sadržaja, metode analize i sinteze, metode dokazivanja, kao i eksperimentalne metode.

Primenom istorijskog metoda pribavljeni su rezultati istraživanja drugih autora koji su se bavili problematikom vezanom za tematiku od interesa. Pribavljeni podaci potiču uglavnom iz eminentnih naučnih radova i istraživanja u ovoj oblasti.

Metoda kompleksnog posmatranja i analiza sadržaja primenjena je prilikom obrade rezultata preuzetih iz istraživanja drugih istraživača. Rezultati su upotrebljeni u cilju definisanja nedostataka postojećih algoritama i utvrđivanja pravaca za potencijalna unapređenja.

Osnovni izazov koji je ovom doktorskom disertacijom rešen dobijen je kroz teorijsku analizu tajnosti i analizu praktičnih primena.

U cilju provere efektivnosti i efikasnosti predloženih rešenja, izvršene su simulacije koje su potvrdile inicijalne hipoteze disertacije.

3.4. Primenljivost ostvarenih rezultata

Zahvaljujući svojoj fleksibilnosti, analitičkoj preciznosti i niskim infrastrukturnim zahtevima, rezultati disertacije imaju širok spektar potencijalnih primena, kako u akademskim istraživanjima, tako i u praktičnoj implementaciji bezbednosnih sistema u uslovima koji zahtevaju robusnu, autonomnu i efikasnu zaštitu tajnosti. Zato rezultati ove disertacije imaju značajnu praktičnu i teorijsku primenljivost u više oblasti informacionih i komunikacionih tehnologija, posebno u kontekstu informacione bezbednosti, kriptografije, sigurne komunikacije i niskonivoske zaštite podataka. Ključne primene mogu se grupisati u sledeće oblasti:

- Sigurna govorna komunikacija u realnom vremenu

Predloženi sistem omogućava izgradnju autonomnih kriptografskih sistema koji ne zavise od složenih infrastrukturnih rešenja za distribuciju ključeva (npr. PKI sistema), već oslanjaju bezbednost na lokalno generisane izvore zajedničke slučajnosti i efikasne IR (Information Reconciliation) protokole, što omogućava: bezbednu end-to-end komunikaciju u uslovima ograničenih resursa (mobilne mreže, vojni uređaji, hitne službe); rešava problem distribucije i zamene tajnih ključeva u dinamičnim okruženjima.

- Sistemi za bezbednost na fizičkom sloju (Physical Layer Security)

IZS konstruisan korišćenjem lokalnih pseudoslučajnih generatora i nezavisnih izvora slučajnosti može se primeniti u komunikacionim kanalima nižeg nivoa (fizički sloj). Time se postiže: robustna zaštita protiv pasivnog prisluškivanja na radijskim kanalima (npr. 5G, IoT, WiFi); Izgradnja nekriptografskih protokola sigurnosti koji zavise od karakteristika komunikacionog kanala, a ne samo od algoritamske složenosti.

- Kvantna i post-quantna bezbednost

Iako sistem nije kvantni, struktura koju koristi – izgradnja zajedničke slučajnosti i korelisanih sekvenci, a zatim njihova destilacija – direktno je inspirisana i kompatibilna sa protokolima kvantne distribucije ključeva (QKD). Zbog toga predloženi SKD protokoli

(posebno WINNOW) mogu se adaptirati u QKD okruženju; modeli evaluacije bezbednosti putem ekvivokacije imaju potencijal za upotrebu u post-kvantnim scenarijima, gde tradicionalna algoritamska sigurnost više nije dovoljna.

- Implementacija u resursno ograničenim sistemima (IoT, SCADA, ugradni sistemi)

Pošto predloženi pristup ne zahteva složenu infrastrukturu i omogućava generisanje ključeva lokalno i deterministički, sistem se lako može integrisati u Internet stvari (IoT) uređaje koji često imaju ograničen procesorski kapacitet i nemaju pristup kvalitetnim hardverskim generatorima entropije; industrijske kontrolne sisteme (SCADA) koji zahtevaju stabilnu bezbednost u realnom vremenu bez oslanjanja na treće strane; vojne i bezbednosne sisteme u kojima je nezavisnost od infrastrukture kritična.

- Kriptografska infrastruktura za zatvorene sisteme i specijalne namene

U specifičnim aplikacijama gde nije moguće ili nije poželjno koristiti javne ključeve i PKI infrastrukture (npr. vojne, diplomatske, vladine mreže), sistem koji koristi samo unapred deljeni ključ i lokalnu slučajnost omogućava; potpuno izolovane sisteme bezbedne komunikacije, nezavisne od interneta, sisteme koji se mogu pokrenuti izvan mreže, uz očuvanje kriptografske sigurnosti.

3.5. Ocena dostignutih sposobnosti kandidata za samostalni naučni rad

Kandidat je u svom dosadašnjem radu pokazao kvalitete presudne za uspešan istraživački rad: sposobnost uočavanja problema i postavljanje korektnog cilja istraživanja, identifikovanje hipoteza, shvatanje i proširivanje teorijskih koncepata, originalnost, sposobnost da teorijske metode pretoči u algoritme, kao i da kritički analizira dobijene rezultate.

4. OSTVARENI NAUČNI DOPRINOS

4.1. Prikaz ostvarenih naučnih doprinosa

Navešćemo naučne doprinose koji predstavljaju direktan doprinos napretku informaciono-teorijske kriptografije, kao i primenjenoj bezbednosti u realnim sistemima. Disertacija ne samo da unapređuje teorijske modele, već istovremeno pruža konkretna rešenja spremna za implementaciju u bezbednosnim arhitekturama koje zahtevaju autonomiju, efikasnost i pouzdanost, analizu i sveobuhvatne simulacije potvrđuju unapređenje performansi u pogledu robusnosti, skalabilnosti i brzini konvergencije, projektovanje transformabilnog i adaptivnog IZS modela zasnovanog na Mauer-ovom principu.

Jedan od najvažnijih doprinosa disertacije jeste definisanje novog tipa izvora zajedničke slučajnosti koji se ponaša funkcionalno ekvivalentno Mauer-ovom satelitskom modelu, ali uz dodatnu parametarsku fleksibilnost. Ovaj IZS se može podešavati u skladu sa uslovima rada sistema (npr. šum, latencija, ograničenja u komunikaciji) i time omogućava dinamičko balansiranje između sigurnosti i performansi. Model podržava: promenljive režime rada (npr. različite brzine generisanja ključeva); kontrolu nad statističkim osobinama izlaznih sekvenci i precizno podešavanje stepena zavisnosti od početnog tajnog ključa i lokalne slučajnosti.

Izvođenje analitičkih donjih granica za ekvivokaciju tajnog ključa pod javnim posmatranjem u prisustvu pasivnog napadača koji ima pristup svim javnim informacijama je jedan od ostvarenih rezultata. Ove granice su izvedene kao funkcije sistemskih parametara i modela sinteze IZS, čime se po prvi put omogućava: formalna kvantifikacija minimalne sigurnosti sistema bez potrebe za empirijskim simulacijama; evaluacija ranjivosti sistema na osnovu njegovih strukturnih osobina i proaktivno projektovanje SKD protokola sa unapred poznatim bezbednosnim granicama.

4.2. Kritička analiza rezultata istraživanja

Rezultati ove disertacije predstavljaju značajan teorijski doprinos razvoju bezbednosnih sistema baziranih na izvorima zajedničke slučajnosti i sekvencijalnoj destilaciji ključeva. Predloženi model je matematički utemeljen, fleksibilan i dizajniran za visok stepen bezbednosti, čak i u neprijateljskim okruženjima.

Postoji potreba za kritičko preispitivanje u praktičnoj primeni, kao i potreba za dodatnim eksperimentalnim proverama. Prelazak sa teorijskog modela na operativne prototipe zahtevaće integraciju sa postojećim kriptografskim standardima, evaluaciju u realnim mrežnim uslovima i proširenje zaštite na aktivne bezbednosne pretnje. Sve ovo ukazuje i na moguće pravce za budući rad.

4.3. Verifikacija naučnih doprinosa

Naučni doprinosi disertacije verifikovani su sledećim radovima kandidata:

Rad u vodećem međunarodnom časopisu kategorije M21a+:

Dejan Cizelj, Milan Milosavljević, Jelica Radomirović, Nikola Latinović, Tomislav Unkašević, Miljan Vučetić, "Synthesis of Sources of Common Randomness Based on Keystream Generators with Shared Secret Keys", *Mathematics*, 2025, 13, 2443. <https://doi.org/10.3390/math13152443>

Rad u nacionalnom časopisu kategorije M52:

Dejan Cizelj, Tomislav Unkašević, Zoran Banjac, "eHealthcare system data privacy concept based on blockchain technology", *Vojnotehnički glasnik*, 2023, vol. 71, br. 4, str. 996-102, 20237. <https://doi.org/10.5937/vojteh71-45589>

Objavljeni radovi u zbornicima međunarodnih konferencija kategorije M33:

Dejan Cizelj, Tomislav Unkasevic, Zoran Banjac, "E-Healthcare Security Concept Based on PKI and Blockchain Technology", *Sinteza* 2023, May 2023. <https://doi.org/10.15308/Sinteza-2023-85-93>

Dejan Cizelj, Miloš Pavlović, Tomislav Unkašević, Zoran Banjac, "Automated Target Tracking Activation Based on Motion Detection", In *Proceedings of X International Conference IcETAN*, East Sarajevo, B&H, 05 - 08.06.2023

Master rad:

Dejan Cizelj, B.; Blokčejn, doprinos sigurnosti informacijama i primene u zdrastvu, master rad, Bijeljina, 2022.

4.4. Preklapanje teksta

Proverom doktorske disertacije utvrđeno je da stepen podudarnosti iznosi 3%. Ovaj rezultat se nalazi značajno ispod dozvoljenih granica i u potpunosti zadovoljava akademske standarde, čime se potvrđuje da je rad originalan i samostalno napisan. Preklapanja su manja od 1% po pojedinim radovima i referencama i odnose se na pojmove i definicije. Ne postoji nijedan pasus da se poklapa sa nekim iz literature.

5. MIŠLJENJE KOMISIJE I PREDLOG

Na osnovu izloženog, komisija konstatuje da doktorska disertacija Dejana Cizelja master računarstva i informatike, pod naslovom „*Sinteza efikasnih izvora zajedničke slučajnosti za potrebe generisanja i distribuciju tajnih kriptografskih ključeva*“ ispunjava sve formalne i suštinske uslove predviđene Zakonom o visokom obrazovanju, kao i propisima Univerziteta Singidunum u Beogradu. Doktorska disertacija Dejana Cizelja sadrži naučne doprinose koji se sastoje u razvoju teorijskih modela u kriptografskim sistemima za savršeno tajni sistem prenosa govora, čiji je sastavni deo podsistem za generisanje i distribuciju potrebne količine tajnih ključeva u realnom vremenu.

Tokom celokupne izrade doktorske disertacije, kandidat je pokazao nesumnjivu sposobnost za samostalni naučnoistraživački rad. Stoga članovi Komisije sa zadovoljstvom predlažu Veću departmana za posle diplomanske studije da se doktorska disertacija kandidata Dejana Cizelja, mastera računarstva i informatike prihvati, izloži na uvid javnosti i uputi na konačno usvajanje Senatu Univerziteta Singidunuma u Beogradu.

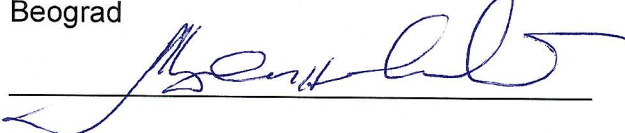
Beograd, 27. 08. 2025. godine

Članovi komisije:

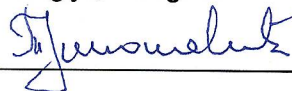
Prof. dr Miljan Vučetić, mentor,
Redovni profesor, Univerzitet Singidunum,
Beograd; Naučni savetnik, Vlatacom institut
visokih tehnologija, Beograd



Prof. dr Mladen Veinović,
Redovni profesor, Univerzitet Singidunum,
Beograd



Dr Tomislav Unkašević,
Naučni saradnik, Vlatacom institut visokih
tehnologija, Beograd



Dr Branko Kovačević,
Profesor emeritus, ETF, Beograd



