VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE
UNIVERZITETA SINGIDUNUM

Beograd
Danijelova 32

Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj: 4-167/2016 od 16.05.2016. godine, određeni smo za članove Komisije za pregled, ocenu i usmenu odbranu doktorske disertacije Slaviše Nikolića, master pod nazivom: "*Nova klasa generatora slučajnih nizova zasnovana na zvučnoj kartici*".

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

REFERAT

1. UVOD

1.1 Hronologija odobravanja i izrade disertacije

Slaviša Nikolić je upisao doktorske studije na Singidunum univerzitetu školske 2010/2011. godine. Položio je svih 12 ispita, sa srednjom ocenom 10. Zahtev za odobravanje teme za izradu doktorske disertacije podneo je 2016. godine. Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj: 4-167/2016 od 16.05.2016. godine, formirana je Komisija u sastavu:

1. dr Mladen Veinović, redovni profesor, Univerzitet Singidunum, Beograd
2. dr Milan Milosavljević, redovni profesor, Univerzitet Singidunum, Beograd
3. dr Branko Kovačević, redovni profesor, Elektrotehnički fakultet, Beograd

za ocenu teme i podobnosti kandidata za izradu doktorske disertacije pod nazivom: "*Nova klasa generatora slučajnih nizova zasnovana na zvučnoj kartici*". Na osnovu pozitivnog izveštaja Komisije Senat Univerziteta Singidunum je 2016. godine odobrio rad na izradi doktorske disertacije. Za mentora je imenovan prof. dr Mladen Veinović. Završnu verzija doktorske disertacije u elektronskom i štampanom obliku Slaviša Nikolić je predao Univerzitetu 29. 07. 2016. godine.

1.2. Naučna oblast disertacije

Tema disertacije kandidata je u oblasti zaštite sistema i podataka, za koju je Fakultet za informatiku i računarstvo Univerziteta Singidunum matičan.

1.3. Biografski podaci o kandidatu

Slaviša Nikolić rođen je 13.11. 1962 godine u Prištini gde je završio osnovnu i srednju elektrotehničku školu i stekao zvanje elektrotehničar za emisione uređaje i primopredajnike.

Zvanje diplomirani inženjer elektrotehnike stekao je 1993 godine na 5-godišnjim akademskim studijama Elektrotehničkog fakulteta u Prištini na smeru elektronika.

Poslediplomske studije na studijskom programu Napredni sistemi zaštite, Univerziteta Singidunum, upisao je školske 2010/2011 godine.

Svoju profesionalnu karijeru započeo je u RMHK Trepča 1990 godine na mestu rukovodioca Elektronskog Računskog Centra. Od 1998. do 2005 godine radio je na mestu sistem inženjer za DATC u komandi Prištinskog korpusa vojske Jugoslavije. Od 2010 godine radi kao profesor stručnih predmeta u Elektrotehničkoj školi „Rade Končar" u Beogradu a od 2011godine u Elektrotehničkoj školi „Zemun" predaje predmete *serveri, računari i programiranje i obrada i prenos signala.*

Objavio je pet rada u međunarodnim naučnim časopisima (od toga dva u časopisima sa SCI liste i tri u zbornicima sa međunarodnih naučnih konferencija).

Njegova trenutna istraživačka interesovanja orijentisana su na bezbedost podataka, informacione i komunikacione tehnologije, komunikaciju i obradu signala, računarske mreže i kriptografiju.

2. OPIS DISERTACIJE

2.1. Sadržaj disertacije

Doktorska disertacija pod naslovom: "*Nova klasa generatora slučajnih nizova zasnovana na zvučnoj kartici*" ima ukupno (14+125) strana. Disertacija ima šest poglavlja i spisak literature. Poglavlja su:

1. Uvod, 7 strana
2. Slučajni nizovi, 25 strana
3. Zvučna kartica i zvuk buke u životnoj sredini, 36 strana
4. Generatori slučajnih nizova, 21 strana
5. Primena metode MiBiS&XOR u postupku destilacije slučajnih nizova, 18 strana
6. Zaključak, 3 strane.

U disertaciji ima ukupno 46 slika, 14 tabela i 110 numerisanih izraza. Literatura sadrži 148 biblografskih jedinica.

2.2. Kratak prikaz pojedinačnih poglavlja

U uvodu su prikazane ideje koje su motivisale istraživački rad na temi disertacije. Istaknuta je aktuelnost teme i dat presek do sada objavljenih rezultata u ovoj oblasti. Ukazano je na nedostatke kod postojećih generatora istinski slučajnih brojeva i potrebe za slučajnim brojevima kao i na prednosti pristupa korišćenog u tezi zasnovanog na zvučnoj kartici. Navedeni su originalni naučni doprinosi teze i kratak pregled preostalih poglavlja.

Drugo poglavlje je organizovano u dva dela. U prvom delu date su osnovne karakteristike šuma sa kojim se srećemo na ulazu generatora istinski slučajnih brojeva sa naglaskom na slučajne procese prirodnih fizičkih izvora slučajnosti. Drugi deo daje opis karakteristika slučajnih signala

i njihovo matematičko predstavljanje. Pažnja je posvećena teoriji verovatnoće sa pregledom apsolutno neprekidnih raspodela neophodnih za razumevanje procesa rada generatora istinski slučajnih nizova. Pored toga uveden je pojam entropije kao mere neizvesnosti i dat je opis entropije složenih sistema. Posebna pažnja posvećena je uvođenju pojma stohastičkih izvora zračenja, kao izvora slučajnosti i karakteristikama slučajnih signala.

Slučajni signal šuma buke u životnoj sredini i struktura hardverskih komponenata korišćenih u ovom radu (zvučna kartica i mikrofon), uvedene su u trećem poglavlju. Opisane su karakteristike zvuka buke u životnoj sredini u frekvencijskom domenu, nivoi buke kao i instrumenti za merenje buke.

Originalni naučni rezultati kandidata prikazani su u četvrtom i petom poglavlju. U četvrtom poglavlju prikazani su generatori slučajnih brojeva, njihova klasifikacija, potreba za generatorima istinski slučajnih brojeva i njihovi najnoviji dizajni. Pokazano je da su razvijeni i primenjeni modeli generatora istinski slučajnih brojeva efikasniji od najčešće korišćenih aplikativnih generatora pseudoslučajnih brojeva i da je njihova upotreba nezamenljiva u jakim kriptografskim i kriptoanalitičkim izazovima. Pored toga u okviru ovog poglavlja prikazan je princip rada generatora istinski slučajnih brojeva sa fazama u njegovom radu kao i različite tehnike post-procesiranja, njihova efikasnost, prednosti i mane.

U petom poglavlju, centralnom delu disertacije prikazani su najvažniji naučni doprinosi kandidata. U prvom delu prikazan je novi način poboljšavanja karakteristika slučajnog niza dobijenog na izlazu ADC konvertora zvučne kartice računara mešanjem bita u koracima čiji rezultat predstavlja odličnu osnovu za drugi deo post-procesiranja koji se izvodi XOR-ovanjem susednih bita u novodobijenom nizu. U drugom delu prikazani su rezultati dobijeni primenom metode MiBiS&XOR, provera tih rezultata primenom statističkih testova slučajnosti i poboljšanja koja se dobijaju. Posebno mesto zauzima značaj i razvoj novog postupka dobijanja istinski slučajnih nizova u cilju dobijanja nove klase generatora koji su brzi, efikasni i jeftini a samim tim i pristupačni širokom auditorijumu. Pokazano je da je prikazani sitem efikasan jer omogućava brzo generisanje slučajnih vrednosti uz zadovoljavajuću nepredvidljivost i da je stoga, iako namenjen u kriptografske svrhe, veoma pogodan za primenu u raznim oblastima od simulacija do igara na sreću.

U zaključku teze su navedeni osnovni doprinosi disertacije i date su smernice za moguća dalja istraživanja u ovoj oblasti.

3. OCENA DISERTACIJE

3.1. Savremenost i originalnost

Istraživanja u oblasti razvoja novih postupaka za generisanje slučajnih nizova su danas veoma aktuelna i usmerena su ka projektovanju i realizaciji fizičkih generatora slučajnosti, kao i u pravcu iznalaženja efikasnih modela za njihovo post-procesiranje i dobijanje što kvalitetnijih istinski slučajnih brojeva. Poseban problem u praksi čine stohastički izvori šuma čije je zračenje slučajnog karaktera i zbog čije prirode, kao i samog principa rada fizičkih generatora, generisanje slučajnih brojeva nije dovoljno brzo. Kandidat je razvio pristup zasnovan na korišćenju zvučne kartice na koju se dovodi signal buke životne sredine kao i novog postupka post-procesiranja i ukazao na prednosti u odnosu na do sada korišćene pristupe.

U ovom kontekstu, kandidat je svoju originalnost potvrdio na korektan i uverljiv način-objavljivanjem radova u međunarodnim naučnim časopisima (5 rada, od čega dva u časopisima sa impakt faktorom) i u zbornicima sa međunarodnih i domaćih naučnih konferencija (3 rada).

3.2. Osvrt na referentnu i korišćenu literaturu

U izradi disertacije korišćena je obimna literatura iz slučajnih procesa i slučajnih signala kao i generatora slučajnih brojeva polazeći od fundamentalnih referenci, pa sve do najnovijih radova u vrhunskim međunarodnim naučnim časopisima. Na osnovu tih referenci, originalni naučni rezultati do kojih je kandidat došao u disertaciji su stavljeni u korektan kontekst.

3.3. Opis i adekvatnost primenjenih naučnih metoda

Kandidat je u svom istraživačkom radu koristio više različitih postupaka. Najpre je uvidom u literaturu, zajedno sa mentorom došao do zaključka o potrebi za razvojem novih efikasnih modela i pristupa za generisanje istinski slučajnih brojeva pomoću računara. Detaljnom analizom raspoloživog hardvera uočeni su nedostaci, sagledane su potencijalne mogućnosti i formulisan je cilj istraživanja: razvoj i promocija novih postupaka generisanja istinski slučajnih brojeva koji su zasnovani na korišćenju zvučne kartice računarskog sistema.

U postupku razvoja nove klase generatora slučajnih nizova, kandidat je pokazao samostalnost i inventivnost u izboru arhitekture generatora, određivanju optimalne strukture i osmišljavanju algoritma za post-procesiranje kao i u pogledu izbora testova i samog testiranja dobijenih rezultata. Razvijeni model generatora slučajnih nizova verifikovan je testiranjem relevantnim statističkim testovima i poređenjem sa odgovarajućim referentnim vrednostima.

Prednosti i nedostaci predloženog pristupa na bazi zvučne kartice su kritički sagledani i na kraju disertacije su date smernice za moguća dalja istraživanja.

3.4. Primenljivost ostvarenih rezultata

Rezultati do kojih je kandidat došao u svojoj disertaciji mogu imati neposrednu primenu u čitavom spektru oblasti uključujući kriptografiju, simulacije, igre na sreću, uzorkovanje, donošenje odluka, medicinu i estetiku, kao i umetnost. Naime, razvijeni modeli generatora odlikuje se velikom brzinom, nepredvidljivi su, nemaju periodičnu zavisnost i finansijski su pristupačni tako da su, iako namenjeni u kriptografske svrhe, pogodni za široku primenu u raznim oblastima. Koristeći predloženi model korisnici kućnih računara mogu generisati kriptografski sigurne slučajne brojeve bez potrebe za ugradnjom ili korišćenjem nekog specijalnog hardvera.

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, shvatanje i proširivanje teorijskih koncepata, originalnost, sposobnost da teorijske metode pretoči u algoritme, strukture podataka i računarske programe, kao i da kritički analizira dobijene rezultate.

4. OSTVARENI NAUČNI DOPRINOS

4.1. Prikaz ostvarenih naučnih doprinosa

Originalni naučni doprinosi disertacije se mogu formulisati na sledeći način:

- Razvoj novog postupka za dobijanje slučajnih brojeva korišćenjem šuma buke životne sredine. Prikazan je efikasan način dobijanja slučajnih bita mešanjem bita ulaznog niza a zatim XOR-ovanjem susednih bita prethodno dobijenog niza slučajnih bita, kod koga je razmeštaj bita takav da su susedni biti udaljeni jedni od drugih, nakon čega se kao rezultat dobija novi niz istinski slučajnih bita i povećava ukupna entropija bitskog niza,
- Razvoj nove klase generatora slučajnih brojeva sposobnih da u kratkom vremenskom roku obezbede značajnu količinu istinski slučajnih brojeva. Testiranja su pokazala da ova klasa generatora ima odlične karakteristike i da generiše istinski slučajne brojeva visokog kvaliteta slučajnosti,
- Razvoj novog postupka korišćenja zvučne kartice, koja je sastavni deo standardnog hardvera personalnih desktop računara ili novijih generacija lap topova, tableta ili mobilnih smart telefona, na koju se preko mikrofona dovodi slučajni analogni signal buke životne sredine u cilju dobijanja nizova istinski slučajnih brojeva koji ispunjavaju sve potrebne karakteristike slučajnosti,
- Doprinos razvoju proceduralnog okruženja i sofverske osnove za dalji proces destilacije slučajnih brojeva kod generatora istinski slučajnih brojeva i za podršku razvoju i unapređenju generatora slučajnih nizova.

Predloženi generatori slučajnih nizova su nepredvidljivi, efikasni, obezbeđuju visok kvalitet slučajnih bita i veliku brzinu generisanja i kao takvi veoma su pogodni za primenu u realnom vremenu. Performanse navedenih generatora verifikovane su testiranjem statističkim FIPS i NIST testovima slučajnosti i poređenjem sa rezutatima poznatih metoda post-procesiranja

4.2. Kritička analiza rezultata istraživanja

U prvoj fazi kandidat je razmatrajući raspoloživu literaturu u oblasti teme disertacije izvršio kritičku analizu dostupnih informacija i korektno definisao cilj istraživanja. U istraživačkom radu koristio je mogućnost kritičkog preispitivanja i pogodne načine verifikacije dobijenih rezultata. Svi razvijeni modeli generatora verifikovani su poređenjem rezultata modelovanja sa odgovarajućim referentnim vrednostima (eksperimentalnim ili rezultatima računarskih simulacija). Uočene su i prikazane prednosti i nedostaci predloženog pristupa i ukazano na smernice mogućih daljih istraživanja.

4.3.Verifikacija naučnih doprinosa

Naučni doprinosi disertacije verifikovani su sledećim radovima kandidata:

Kategorija M23

1. **Slaviša Nikolić**, Mladen Veinović: "Advancement of true random number generators based on sound cards through utilization of a new post-processing method", *Wireless Personal Communications*, pp. 1-20, DOI 10.1007/s11277-016-3480-9, ISSN 0929-6212, E ISSN 1572-834X, Springer US.

Kategorija M33

1. **Slaviša Nikolić**: "A new method of distillation of True Random Pulse Generators based on sound card", April 2014 Conference: Sinteza - Medjunarodna konferencija Univerziteta Singidunum, At Belgrade, Serbia, Volume: Data security, DOI: 10.15308/Sinteza-2014-995-1000.
2. **Slaviša Nikolić**, Dejan Uljarević: "Design of a true random number generator using environmental noise", April 2015 Sinthesis-International Scientific Conference of IT and Business-Related Research, Volume: Information security and cryptographic applications, DOI: 10.15308/Synthesis-2015-97-100.

Kategorija M53

1. Dejan Tepšić, Mladen Veinović, Aleksandar Mišković, **Slaviša Nikolić**: "Impact of security protocols on performance in IEEE 802.11 wireless networks", Accepted for publishing in TTEM Journal Technics, Technologies, Education and Management 12/2013; 8(4):1757-1765

Kategorija M63

1. **Slaviša Nikolić**, Mladen Veinović: "Jedna realizacija generatora istinski slučajnih impulsa na bazi zvučne kartice računara", January 2013 Conference: 12. Međunarodni naučni skup Sinergija 2013, At Bijeljina, BiH, Volume: Informacioni sistemi, Bezbednost i zaštita, Tehničke nauke i logistika.

5. MIŠLJENJE KOMISIJE I PREDLOG

Na osnovu izloženog, komisija konstatuje da doktorska disertacija Slaviše N. Nikolića, pod naslovom "*Nova klasa generatora slučajnih nizova zasnovana na zvučnoj kartici*" ispunjava sve formalne i suštinske uslove predviđene Zakonom o visokom obrazovanju, kao i propisima univerziteta Singidunum u Beogradu. Doktorska disertacija Slaviše Nikolića sadrži naučne doprinose koji se sastoje u razvoju efikasne klase generatora istinski slučajnih nizova zasnovane na zvučnoj kartici koji se uspešno primenjuju u postupcima generisanja istinski slučajnih brojeva i novog postupka post-procesiranja koji se može primeniti i kod drugih vrsta generatora slučajnih nizova.

Tokom celokupne izrade doktorske disertacije kandidat je pokazao nesumnjivu sposobnost za samostalni nauučnoistraživački rad. Stoga članovi Komisije sa zadovoljstvom predlažu Veću departmana za poslediplomske studije i medjunarodnu saradnju da se doktorska disertacija pod

naslovom "*Nova klasa generatora slučajnih nizova zasnovana na zvučnoj kartici*" kandidata Slaviše N. Nikolića izloži na uvid javnosti i uputi na konačno usvajanje Senatu univerziteta Singidunuma u Beogradu.

Beograd, 22. 08. 2016. godine

Članovi komisije:

dr Mladen Veinović, redovni profesor,
Univerzitet Singidunum, Beograd

dr Milan Milosavljević, redovni profesor,
Univerzitet Singidunum, Beograd

dr Branko Kovačević, redovni profesor,
Elektrotehnički fakultet, Beograd