UNIVERZITET SINGIDUNUM
Departman za poslediplomske studije
Danijelova 32, Beograd

VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE

Odlukom Veća Departmana za poslediplomske studije broj 4 – 115/2021 od 25.05.2021. godine određeni smo za članove Komisije za ocenu i odbranu doktorske disertacije kandidata Tomislava Unkašević **"Sinteza jedne klase pouzdanih kriptografskih algoritama za sisteme sa ograničenim resursima"**, o čemu podnosimo sledeći

IZVEŠTAJ

1 Osnovni podaci o kandidatu i doktorskoj disertaciji

Tomislav Unkašević je rođen 01.09.1960. godine u Zemunu gde je završio osnovnu školu. U Beogradu je pohađao i završio Matematičku gimnaziju sa odličnim uspehom. Na Matematičkom fakultetu Univerziteta u Beogradu diplomirao je 1985. godine sa prosečnom oceno 9.12. U toku treće i četvrte godine studija primao je stipendiju Srpske akademije nauka i umetnosti namenjenu talentovanim studentima matematike.

Doktorske akademske studije na studijskom programu Napredni sistemi zaštite na Univerzitetu Singidunum, upisao je školske 2018/2019. godine.

Zaposlen je u Institutu VLATACOM kao istraživač na projektima vezanim za bezbednost podataka i informacionih sistema.

Njegova istraživačka interesovanja se odnose na kriptologiju, analizu i sintezu kriptografskih algoritama, analizu bezbednosnih protokola, bezbednost informacionih sistema, dizajn i analizu algoritama i diskretnu matematiku.

Govori, čita i piše engleski jezik i služi se ruskim jezikom.

Kandidat ima sledeći objavljen rad kategorije M21 čime je ispunjen preduslov za odbranu doktorske disertacije.

[1] ***Unkašević, T.,*** *Banjac. Z. and Milosavljević, M. (2019), "Generic Model of the Pseudo-Random Generator Based on Permutations Suitable for Security Solutions in*

Computationally-Constrained Enviroments", Sensors, ISSN 1424-8220, Volume 19, Issue 23, December 2019, article 5322, DOI: ***https://doi.org/10.3390/s19235322****, IF: 3,031, M21*

Objavljeni radovi u časopisima kategorije M21

[1] *Livada, B., Vujić. S., Radić, D.,* ***Unkašević, T.*** *and Banjac. Z. (2019), "Digital magnetic Compass Integration with Stationary, Land-Based Electro-Optical Multi-Sensor Surveillance System", Sensors, ISSN 1424-8220, Volume 19, Issue 19, October 2019, article 4331, pp. 433101-4331018, DOI: 10.3390/s19194331, IF: 3,031, M21*

Preostali objavljeni radovi:

Objavljeni radovi u vodećim nacionalnim časopisima kategorije M 51

[1] *J. Polajnar* ***T. Unkašević*** *"Equitable Probabilistic Elections in Ring Networks" YUJOR, VOL.4 1994 Beograd*

Objavljeni radovi na međunarodnim konferencijamakategorije M33

[1] ***T.Unkašević****, M.Marković, G.Đorđević, Optimization of RSA algorithm implementation on TI TMS320C54x Signal Processors Based on a Modified Karatsuba-Offman's algorithm, ECMCS'2001, 11-13 September, 2001, Budapest.*

[2] ***T.Unkašević****, M.Marković, G.Đorđević, "Optimization of RSA Algorithm Implementation on TI TMS320C54x Signal Processors," in Proc. of TELSIKS'2001, September 19-21, 2001, Niš, pp. 603-606.*

[3] *G.Đorđević,* ***T.Unkašević****, M.Marković, "Optimization of Modular Reduction Procedure in RSA Algorithm Implementation on Assembler of TMS320C54x Signal Processors," DSP 2002, July, 2002, Santorini, Greece.*

[4] *M.Marković,* ***T.Unkašević****, G.Đorđević, "RSA Algorithm Optimization on Assembler of TI TMS320C54x Signal Processors," EUSIPCO 2002, Toulouse, France, Sept. 3-6, 2002.*

[5] *Goran Đorđević,* ***Tomislav Unkašević****, Milan Marković, "Influence of Key Length in Possible Optimization of RSA Algorithm Implementation on Signal Processor," in Proc. ICEST 2002, Niš, Yugoslavia, Oct. 1-4, pp. 23 – 26.*

[6] *G.Đorđević, M.Marković,* ***T.Unkašević****, "Neki aspekti implementacije IDEA algoritma na signal procesorima TI TMS320C54x familije," Zbornik radova IX Telekomunikacionog foruma, TELFOR 2001, Novembar 20-22, 2001, pp. 431-434.*

[7] *G.Đorđević,* ***T.Unkašević****, M.Marković, "O mogućim efikasnim realizacijama AES algoritma na signal procesorima TI TMS320C54x familije," Zbornik radova XLVI Konf. ETRAN, Banja Vrućica, Teslić, 4-7 jun, 2002, tom 1, pp. 122-125.*

[8] *M.Marković, G.Đorđević,* ***T.Unkašević****, "On Optimizing RSA Algorithm Implementation on Signal Processor Regarding Asymmetric Private Key Length", in Proceedings of WISP 2003, Budapest, Sept. 2003, pp. 73-77.*

[9] *Milan Marković, Goran Đorđević,* ***Tomislav Unkašević****, "Mogućnost implementacije provere prostoće velikih brojeva na TI TMS320C54x signal procesorima", ETRAN, Herceg Novi, Jun 2003.*

[10] ***T.Unkašević****, M.Marković, G.Đorđević, O mogućnostima optimizacije kriptografskih algoritma implementiranih na digitalnim signal procesorima TITMS C54X familije,Zbornik radova ETRAN 2005, Herceg Novi 2005. National conference proceedings*

[11] *Milosav, P., Banjac, Z., Milosavljević, M.,* ***Unkašević, T.****, and Mostafa, M.A.M (2019), "Overview and Classification of Digital Watermarking Algorithms", International Scientific Conference on Information Technology and Data Related Research SINTEZA 2019, Novi Sad, April 20 2019.M33*

[12] ***Unkašević, T.****, Banjac, Z., Milosavljević, M., Milosav, P., and Mostafa, M.A.M , "Contribution to the theory and practice of generating RSA algorithm keys", International Scientific Conference on Information Technology and Data Related Research SINTEZA 2019, Novi Sad, April 20 2019.M33*

[13] *Latinovic N., Al-Atrooshi H. A. M.,* ***Unkašević T.****, Perić M., Veinović M., „Bulk Mode Encryption Devices Modification for Usage of Quantum Key Distribution", Proc. of 27th IEEE Telecommunications forum (TELFOR), Belgrade, Serbia, 26 - 27 November 2019, M33*

Objavljeni radovi na domaćim konferencijama kategorije M63

[1] *J. Polajnar,* ***T. Unkašević*** *Đ. Mastilović Razvoj komunikacionih protokola za računarski sistem RACON, ETAN , BLED 1987.*

[2] *J. Polajnar,* ***T. Unkašević*** *Equitable Probabilistic Elections in Ring Networks, SYM-OP-IS '93, Beograd 1993.*

[3] ***T. Unkašević*** *An Efficient Algorithm for Probability Distribution of Series, SYM-OP-IS '94,Kotor 1994.*

[4] ***T. Unkašević*** *Elementaran dokaz o najkraćem rastojanju između dve tačke na sferi, Jugoslovenski geometrijski seminar, Divčibare 1996.*

[5] ***T. Unkašević*** *O jednoj slabosti RSA algoritma i mogućnostima za njenu zloupotrebu, SYM-OP-IS '97,Bečići 1997.*

[6] ***T. Unkašević*** *O karakteristikama jednog pseudoslučajnog generatora, SYM-OP-IS '98,Herceg Novi 1998*

[7] ***T.Unkašević****, M.Marković, G.Đorđević, "O mogućnostima implementacije RSA algoritma na signal procesorima Texas Instruments TMS320C54x familije," Zbornik radova SYM-OP-IS'2000, Beograd, pp. 185-188.*

[8] *G. Đorđević,T. Unkašević, Optimizacija RSA algoritma implementiranog na digitalnim signal procesorima Texas Instruments TMS320C54x familije, INFOFEST, Budva, 2000.*

[9] *G.Đorđević,* ***T.Unkašević****, M.Marković, "Optimizacija implementacije RSA algoritma na Texas instruments signal procesorima primenom kineske teoreme ostataka," Zbornik radova INFOTEH'2001I, Vrnjačka Banja, 18.-22. Jun 2001.*

[10] *G.Đorđević, **T.Unkašević**, M.Marković, "Optimizacija implementacije RSA algoritma na Texas instruments signal procesorima primenom kineske teoreme ostataka," Zbornik radova INFOTEH'2001I, Vrnjačka Banja, 18.-22. Juni 2001.*

[11] *B.Milovanović, G.Đorđević, M.Marković, **T.Unkašević**, "O mogućim efikasnim realizacijama IDEA algoritma na signal procesorima TI TMS320C54x familije," Zbornik radova konferencije IT 2002, Žabljak, 2002.*

[12] *G.Đorđević, M.Marković, **T.Unkašević**, "O poboljšanju efikasnosti implementacije RSA algoritma na TMS320C54x signal procesorima," Zbornik radova YU INFO 2002, Kopaonik, 2002.*

[13] ***T. Unkašević**, O osetljivosti kriptografkih algoritama, DataProtection 2003, Beograd 2003.*

[14] *Goran Đorđević, Milan Marković, Tomislav Unkašević, "O mogućnosti optimizacije realizacije Miler-Rabinovog testa provere prostoće velikih brojeva na TI TMS320C54x signal procesorima " , YUINFO, Kopaonik, Mart 2003.*

[15] *Goran Đorđević, Milan Marković, **Tomislav Unkašević** "Komparativna analiza savremenih javnih simetričnih kriptografskih algoritama ", YUINFO, Kopaonik, Mart 2004.*

[16] ***Tomislav Unkašević** O jednoj osobini višestrukih linearnih pomeračkih registara Zbornik radova SYM-OP-IS'2010, Divčibare.*

[17] *Sonja Kuljanski, **Tomislav Unkašević** O efikasnosti algoritama za verifikaciju statusa sertifikata XLI Simpozijuma o operacionim istraživanjima – SYM-OP-IS 2014 Divčibare*

[18] ***Tomislav Unkašević**, Sonja Kuljanski Uticaj prezentacije brojeva na algoritme za multipr eciznu aritmetiku XLI Simpozijuma o operacionim istraživanjima – SYM-OP-IS 2014 Divčibare.*

[19] ***Томислав Ункашевић**, Мирослав Перић, Зоран Бањац, О осетљивости криптографских система, Зборник радова 23. телекомуникациони форум ТЕЛФОР 2015, DRUŠTVO ZA TELEKOMUNIKACIJE – DT, BEOGRAD, ETF - Elektrotehnički fakultet Univerziteta u Beogradu, IEEE Serbia & Montenegro COM CHAPTER, -1, vol. 23, no. 1, pp. 2.15 - 2.15, issn: 978-1-5090-054-8, udc: 519.2, Србија, 24. - 25. Nov, 2015*

[20] ***Unkašević, T.,** Banjac. Z., Milosavljević, M., Milosav, P. and Al-Atrooshi, H.A.M. (2019), "Generički model pseudoslučajnog generatora baziran na permutacijama", Proc. of 27th IEEE Telecommunications forum (TELFOR), Belgrade, Serbia, 26 - 27 November 2019.M63*

Tehničko rešenje primenjeno na međunarodnom nivou M81

[1] *T. Unkašević, Z. Banjac, M. Perić, D. Čoja, S. Ćirković, Sistem za razmenu kriptografskih ključeva u uređaju za zaštitu govora u mobilnoj telefoniji VE3FA*

Projekti

[1] ***Vlatacom Reliable Communication Channel - high capacity transmission lines encryption,***

[2] ***National Crypto Centre Solution,***

[3] ***Voice Encryption and Three Factor authentication.***

[4] ***RSA key quality verification***

[5] ***eID security***

Doktorska disertacija kandidata Tomislava Unkaševića je urađena na 132 strane, od čega 12 strana čini spisak literature. Spisak literature obuhvata 122 reference koje čine naučni radovi, knjige, zbornici radova i elektronski izvori. Uz osnovni tekst sadrži sedamnaest slika i jednu tabelu.

Doktorska disertacija kandidata Tomislava Unkaševića je bila podvrgnuta proveri softverom za ustanovljavanje preklapanja/plagijarizma (iThenticate Plagiarism Detection Software). Ukupan procentualni iznos zapaženih preklapanja iznosi 9% disertacije.

2 Predmet i cilj istraživanja

Predmet istraživanja je analiza kriptografskih bezbednosnih svojstava sekvencijalnih kriptografskih konstrukcija sa promenljivim permutacija i sinteza efikasnog kriptografskog algoritma pogodnog za uređaje sa ograničenim računarskim resursima

Cilj ovog istraživanja je sinteza klase bezbednih i efikasnih simetričnih sekvencijalnih kriptografskih algoritama za uređaje sa ograničenim resursima i njihovim mrežama. Sinteza se zasniva na modelu promenljivih permutacija. U sklopu procesa sinteze sprovodi se analiza bezbednosnih karakteristika modela promenljivih permutacija. Ispitivanje čine statističke i algebarske analize i predmet ispitivanja su sledeće osobine:

- Analiza raspodele verovatnoća izlaznog niza
- Analiza korelacije između izlaznog niza i elemenata unutrašnjeg stanja kriptografskog algoritma
- Analiza autokorelacija izlaznog niza
- Analiza perioda izlaznog niza
- Algebarska analiza svojstava kriptografskog algoritma

3 Hipotetički okvir istraživanja

Opšta hipoteza od koje se krenulo u istraživanje u disertaciji je: *"Na osnovu do sada poznatih teorijskih znanja i tehnika kriptoanalize pseudoslučajnih generatora moguće je definisati kriptografski pouzdane pseudoslučajne generatore "*

Posebna hipoteza koja proizilazi iz opšte je: *„Moguće je definisati efikasne i kriptografske pseudoslučajne generatore na osnovu promenljivih permutacija sa dobrim*

bezbednosnim karakteristikama koji su pogodni za implementaciju u uređaje sa ograničenim resursima".

H1. Primena promenljivih permutacija omogućava definisanje efikasnog generičkog pseudoslučajnog generatora

H2. Bezbednosne karakteristike definisanog generičkog pseudoslučajnog generatora su dobre u kriptografskom smislu

4 Metodologija istraživanja

Metodologija istraživanja u ovom radu obuhvata složen i organizovan postupak zasnovan na logičkim načelima i strogim matematičkim principima tipičnim za analizu i sintezu kriptografskih mehanizama dokazive bezbednosti. Složenost predmeta istraživanja zahteva primenu:

- analitičkih osnovnih metoda – metod analize, metod apstrakcije, metod specijalizacije i metod dedukcije;
- sintetičkih osnovnih metoda – sintezu, konkretizaciju, generalizaciju i indukciju;
- opšte naučnih metoda – hipotetičko-deduktivnu, analitičko-deduktivnu, komparativnu, matematičku i statističku metodu modelovanja.

Ovaj izbor istraživačkih metoda je upotrebljen da se istraživanje i tok istraživačkog procesa u svim fazama, odnosno identifikaciji i definisanju problema, planiranju dizajna istraživanja, kritičkoj analizi sistema, kao i formulaciji zaključaka korektno sprovede u skladu sa osnovnim principima naučno istraživačkog rada. Primenom ovih metoda, kako pokazuju prezentovani rezultati istraživanja, moguće je validno ostvarenje naučnog i društvenog cilja istraživanja

5 Kratak sadržaj doktorske disertacije

Rad se sastoji iz 5 poglavlja, sadržajno strukturiranih na sledeći način.

U prvom poglavlju, uvodnom razmatranju ukratko je izložena motivacija za ovu disertaciju, problem koji se razmatra, pristup njegovom rešavanju i struktura disertacije.

U drugom poglavlju daje se taksonomija i osnovne karakteristike kriptografskih algoritama, klasifikacija stepena bezbednosti, modeli za procenu njihove bezbednosti i komparativna analiza opisanih modela za procenu bezbednosti kriptografskih algoritama.

U trećem poglavlju se daje pregled i analiza do sada poznatih konstrukcija baziranih na promenljivim permutacijama i njihove bezbednosne karakteristike.

U četvrtom poglavlju koje je centralni deo disertacije daje se opis parametrizovane klase sekvencijalnih kriptografskih algoritama i njemu pridruženi matematički model. U ovom delu je sprovedena analiza bezbednosnih karakteristika predložene konstrukcije i

komparativna analiza dobijenih rezultata sa algoritmima i slabostima opisanim u trećem delu. Analizirane su moguće primene predložene konstrukcije i formulisani zaključci u vezi sa predloženom konstrukcijom.

U petom poglavlju se daje rezime istraživanja, pregled glavnih doprinosa disertacije kao i mogući pravci daljeg istraživanja u ovoj oblasti.

6 Postignuti rezultati i naučni doprinos disertacije

Potvrđeni doprinosi ovog rada su sledeći:

- Definisana je klasa pseudoslučajnih generatora parametrizovana sa dva parametra. Ako se pseudoslučajni generator posmatra kao konačan automat sa izlazom parametri su funkcija promene stanja i funkcija izlaza.
- Kriptografske karakteristike definisane klase u pogledu funkcije raspodele verovatnoća izlaznog niza, perioda izlaznog niza te korelacionih i algebarskih osobina su sa kriptografskog stanovišta dobre.
- Kriptografske karakteristike definisane klase zavise samo od pripadnosti parametara skupu dobrih parametara a ne i od izbora konkretnih vrednosti parametara. Izvedena je karakterizacija skupa i njegova brojnost ukazuje na mogućnost dobijanja praktično beskonačnog broja dobrih uzajamno nekorelisanih pseudoslučajnih generatora.
- Mehanizam promenljivih permutacija omogućava sintezu vrlo efikasnih i kompaktnih pseudoslučajnih generatora primenljivih i u uređajima sa vrlo ograničenim resursima.
- Na izvestan način definisana klasa pseudoslučajnih generatora predstavlja uopštenje generatora RC4 i po prikazanim rezultatima predstavlja rehabilitaciju ove ideje u kriptografskom miljeu.
- Definisanje jedne ovakve klase kriptografskih pseudoslučajnih generatora u zna čajnoj meri unapređuje mogućnosti realizacije različitih, pa i vrlo visokih, nivoa bezbednosti podataka čak i na uređajima sa vrlo ograničenim resursima.
- Bezbednosne karakteristike predložene klase kao i kompaktnost implementacije omogućavaju standardizaciju kriptografskih rešenja za uređaje sa velikim rasponom procesnih mogućnosti.

7 Mišljenje i predlog Komisije o doktorskoj disertaciji

Na osnovu svega izloženog Komisija je mišljenja da doktorska disertacija kandidata Tomislava Unkaševića po svojoj temi, pristupu, strukturi i sadržaju rada, kvalitetu i načinu izlaganja, metodologiji istraživanja, načinu korišćenja literature, relevantnosti i kvalitetu sprovedenog istraživanja i donetim zaključcima zadovoljava kriterijume zahtevane za doktorsku disertaciju, te se može prihvatiti kao podobna za javnu odbranu.

Sagledavajući ukupnu ocenu doktorske disertacije kandidata Tomislava Unkaševića pod nazivom "Sinteza jedne klase pouzdanih kriptografskih algoritama za sisteme sa ograničenim resursima", predlažemo Veću departmana za poslediplomske studije i Senatu

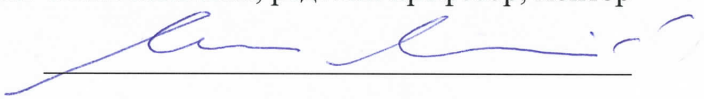
закључцима задовољава критеријуме захтеване за докторску дисертацију, те се може прихватити као подобна за јавну одбрану.

Сагледавајући укупну оцену докторске дисертације кандидата Томислава Ункашевића под називом "Синтеза једне класе поузданих криптографских алгоритама за системе са ограниченим ресурсима", предлажемо Већу департмана за последипломске студије и Сенату Универзитета Сингидунум да прихвати напред наведену докторску дисертацију и одобри њену јавну одбрану

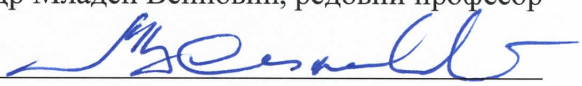
Београд,09.06.2021

Чланови комисије:

проф. др Милан Милосављевић, редовни професор, ментор



проф. др Младен Веиновић, редовни професор



др Бранко Ковачевић, проф. емеритус, Електротехнички факултет Универзитета у Београду