Naučnom veću
Matematičkog instituta SANU

Na XXXII sednici Naučnog veća Matematičkog instituta SANU, održanoj 25. maja 2015. godine, određeni smo u komisiju za izbor dr Irine Branović Balović u zvanje **viši naučni saradnik** i u vezi sa time podnosimo sledeći

IZVEŠTAJ

Dr Irina Branović Balović zaposlena je u Matematičkom institutu SANU od oktobra 2014. godine.

Biografija kandidata

1. Obrazovanje

Irina Branović rođena je 15.02.1975. godine u Zrenjaninu, gde je završila osnovnu školu i gimnaziju. Diplomirala je na smeru za elektroniku Elektrotehničkog fakulteta Univerziteta u Beogradu 2000. godine.

Poslediplomske doktorske studije upisala je 2001. godine kao stipendista Departmana za Informatičko inženjerstvo Univerziteta u Sijeni, Italija. Doktorska istraživanja bila su orijentisana na poboljšanje efikasnosti algoritama za šifrovanje javnim ključem u embedded procesorima. Maja 2005. godine odbranila je doktorsku tezu pod naslovom **"Instruction Set Extensions for Elliptic Curve Cryptography over Binary Finite Fields"**. Doktorat je nostrifikovan na Univerzitetu Singidunum Rešenjem o priznavanju strane visokoškolske ustanove od 23.03.2010.

2. Zaposlenje

Dr Irina Branović provela je period od 2001 - 2005 kao doktorant - stipendista, asistent na Departmanu za Informatičko inženjerstvo Univerziteta u Sijeni, Italija. Tokom boravka na doktorskim studijama bila je angažovana kao asistent na predmetima Arhitektura računara i Operativni sistemi. U ovom periodu uspešno je položila sve predviđene ispite, među kojima je najznačajniji bio kurs Šifrovanje na Institutu IAIK u Gracu 2003. godine, gde je predavač bio Vincent Rijmen.

U periodu 2005 - 2009. godine radila je kao part-time softver inženjer u firmi OpenLab Software Engineering u Firenci, gde je razvijala softver za upravljanje projektima.

Istovremeno je u periodu 2006 - 2008 bila dobitnik stipendije za mlade istraživače regije Toskana i tokom tog perioda razvijala je softver za biometrijsku autentikaciju u saradnji sa firmom Bassnet iz Firence.

Dugi niz godina bavila se prevođenjem strane računarske literature za izdavačku kuću Mikroknjiga, a objavljivala je i autorske članke na tematiku programiranja u časopisu Mikro.

Nakon povratka u Srbiju, u periodu 2010 - 2014 radila je kao docent na Univerzitetu Singidunum u Beogradu, gde je bila angažovana na predmetima Objektno - orijentisano programiranje, Internet tehnologije, Menadžment informacioni sistemi, Napredno Java programiranje. Iz ovog perioda datiraju udžbenici za pomenute predmete koji su i dalje u upotrebi na Univerzitetu Singidunum. Tokom istog perioda bila je saradnik na dva projekta tehničko-tehnološkog razvoja, "Razvoj novih informaciono komunikacionih tehnologija korišćenjem matematičkih metoda sa primenama u medicine, telekomunikacijama, energetici, zaštiti nacionalne baštine i obrazovanju" kojim rukovodi dr Zoran Ognjanović, i "Istraživanje tehničko tehnološke, kadrovske i organizacione osposobljenosti Železnica Srbije sa aspekta tekućih i budućih zahteva Evropske Unije" kojim rukovodi dr Miloš Ivić sa Saobraćajnog fakulteta Univerziteta u Beogradu. U okviru projekta Saobraćajnog fakulteta bavila se problemima rutiranja vozila, raspoređivanja u transportu, kao i usaglašavanjem informatičkih standarda između Železnica Srbije i EU.

Od oktobra 2014. dr Irina Branović angažovana je na Matematičkom Instututu SANU kao saradnik na projektima koje Institut koordinira. Oblasti istraživanja kojima se trenutno bavi su raznorodne i obuhvataju cloud sisteme, energetsku efikasnost, edukaciju u računarstvu, 3D modeliranje. Istovremeno je aktivno angažovana i kao vodeći softver inženjer na različitim komercijalnim projektima.

Bibliografija kandidata - kvantitativni kriterijumi

Spisak naučnih radova za izbor u zvanje viši naučni saradnik

Monografija međunarodnog značaja ($M_{12} = 10$)

1. I. Branovic, Instruction Set Extensions For Elliptic Curve Cryptography: An analysis of instruction set extensions for ECC over binary finite fields in embedded systems, Lambert Academic Publishing, ISBN 978-3-8383-8011-7, 80 strana, 2010. http://www.amazon.com/Instruction-Extensions-Elliptic-Curve-Cryptography/dp/3838380118/ref=sr_1_1?s=books&ie=UTF8&qid=1435085334&sr=1-1&keywords=irina+branovic

   Rezime najvažnijih doprinosa doktorske disertacije. Započinje uvodom u u teoriju brojeva i problematiku šifrovanja eliptičkim krivama, nastavlja se pregledom aritmetike u konačnim poljima i diskusijom različitih metoda implementiranja operacija nad eliptičkim krivama u softveru. Opisan je test

softver razvijen za potrebe procene performansi kriptografskih operacija nad krivama, kao i metodologija izvođenja eksperimenata na simulatoru arhitekture procesora. U nastavku je dat pregled performansi test koda kada se u skup istrukcija ARM procesora dodaju dve nove naredbe. Monografija se zaključuje analizom moguće implementacije aritmetike u konačnim poljima na različitim arhitekturama, te se tako može koristiti i kao vodič za primenu šifrovanja eliptičkim krivama u "pametnim" uređajima.

Poglavlja u monografijama međunarodnog značaja ($M_{14} = 4$)

1. D. Marković, I. Branović, R. Popović, D. Živković, V. Tomasević, Cloud Computing in Business, Chapter in Book Advances in Cloud Computing Research by Nova Science Publishers, ISBN 978-1-63117-193-2, 2014.
https://www.novapublishers.com/catalog/product_info.php?products_id=47968

   Pregledni rad koji opisuje trenutno stanje integracije računarstva "u oblaku" u poslovne procese, razmatra granične teme poput potrošnje energije i emisije ugljen dioksida u energetski efikasnim okruženjima "u oblaku" i predstavlja moguće pravce napredovanja računarstva "u oblaku" u bliskoj budućnosti.

2. D. Marković, I. Branović, R. Popović, Collaborative Learning and 3D Technology, Chapter in Book Collaborative Learning: Theory, Strategies and Educational Benefits by Nova Science Publishers, ISBN 978-1-63321-790-4, 2014.
https://www.novapublishers.com/catalog/product_info.php?products_id=51224

   Pregled virtuelnih kolaborativnih 3D okruženja za edukaciju uz diskusiju faktora koji utiču na njihovo prihvatanje i analizu ključnih faktora za postizanje efikasnog kolaborativnog okruženja. Predložen je inovativan pristup kroz dizajniranje 3D virtuelnih učionica u kojima će kolaborativni pristup edukaciji biti olakšan kroz rad u grupama.

Radovi u vodećim časopisima međunarodnog značaja ($M_{21} = 8$)

1. S. Bartolini, I. Branović, R. Giorgi, E. Martinelli, Effects of Instruction-set Extensions on an Embedded Processor: a Case Study on Elliptic Curve Cryptography over GF(2m), *IEEE Transansactions on Computers*, 57(5):672–685, 2008. (citiran 10 puta)
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4358294

   Rezultati profiliranja i merenja vremena izvršavanja algoritama za šifrovanje eliptičkim krivama u procesorima sa množačem koji koristi aritmetiku u konačnim poljima. Predloženi su optimalan izbor parametara za eliptičke krive, kao i metoda implementacije algoritama u softveru.

2. D. S. Marković, D. Živković, I. Branović, R. Popović, D. Cvetković, Smart Power Grid and Cloud Computing, *Renewable and Sustainable Energy Reviews*, 24: 566–577, 2013. (citiran 31 put)
http://www.sciencedirect.com/science/article/pii/S136403211300227X

   Pregledni rad koji razmatra kako se prednosti računarstva "u oblaku", poput smanjene cene, povećanog prostora za skladištenje i korišćenja "po potrebi" mogu primeniti na razvoj "pametne" električne mreže (engl. smart grid).

Radovi u časopisima međunarodnog značaja ($M_{23} = 3$)

1. V. Milutinovic, I. Branovic, et al, Testing the E-Business Infrastructure: Expanding into the Wireless/Mobile Environments, *Telecommunication Systems*, 22:(1-4):141–150, 2003.
http://link.springer.com/article/10.1023%2FA%3A1023438903896

   Ukazuje na neophodnost nezavisnog testiranja instrastrukture za elektronsko poslovanje u bežičnim okruženjima.

2. I.Franc, I.Stanković, I. Branović, R.Popović, Ontology Based Model of Digital Forensic Virtual Lab and Curriculum Design, *International Journal of Engineering Education*, 30(4):1–13, 2014.
http://www.ijee.ie/covers/covandabs30-4.pdf

   Opisuje ontološki pristup projektovanju kurikuluma za digitalnu forenziku na sva tri nivoa studija i virtuelnu učionicu za digitalnu forenziku razvijenu u okviru ove studije.

3. S. Mladenović, S.Vesković, S. Janković, S. Aćimović, I. Branović, Heuristic Based Real-Time Train Rescheduling System, prihvaćen za objavljivanje, *Networks*, 2015.

   Predlog efikasnog rešenja problema dinamičkog preraspodeljivanja vozova kao odgovor na poremećaje u realnom vremenu primenom heurističkih metoda. Predložena je kombinacija tri klase heuristika, opisani su eksperimenti na železničkoj mreži Beogradskog čvora i predstavljen softver razvijen za automatsko rešavanje konflikata i izbor najpovoljnijeg rešenja za preraspodeljivanje (engl. rescheduling).

Radovi u časopisima nacionalnog značaja ($M_{52} = 1.5$)

1. D. Marković, I. Branović, R. Popović, D. Živković, V. Tomašević, Review of cloud computing in business, pp. 673-677, Singidunum Journal of Applied Sciences, pp. 673-677, ISBN: 978-86-7912-539-2, 2014.

   Preliminarni pregled stanja u razvoju računarstva "u oblaku".

2. S. Janković, S. Mladenović, S. Vesković, I. Branović, Informacioni sistem za podršku odlučivanju na železnici zasnovan na WCF Data servisima, Singidunum Journal of Applied Sciences, pp. 841-845, ISBN: 978-86-7912-539-2, 2014.

   Opis implementacije WCF Data servisa koji iz baze podataka JP Putevi Srbije preuzimaju podatke o prosečnom godišnjem i mesečnom dnevnom saobraćaju po osnovnim vrstama vozila na saobraćajnim deonicama, a dobijeni podaci služe kao sistem za podršku u odlučivanju pri upravljanju bezbednošću saobraćaja na putno-pružnim prelazima.

Radovi u međunarodnim časopisima koji nisu na SCI listi ($M_{53} = 1$)

1. I. Branovic, R Giorgi, E Martinelli, A workload characterization of elliptic curve cryptography methods in embedded environments, ACM SIGARCH Computer Architecture News, 32 (3): 27-34, 2004. (citiran 20 puta)
   http://dl.acm.org/citation.cfm?id=1024299

   Preliminarni rezultati istraživanja performansi šifrovanja eliptičkim krivama u "embedded" arhitekturama i opis originalnih test programa razvijenih za potrebe merenja performansi.

2. D. Marković, I. Branović, R. Popović, Smart Grid and nanotechnologies: a solution for clean and sustainable energy, *Energy and Emission Control Technologies*, Dovepress Publishing, Vol 2, pp. 1-13, 2015.
   http://www.dovepress.com/smart-grid-and-nanotechnologies-a-solution-for-clean-and-sustainable-e-peer-reviewed-article-EECT

   Pregledni rad koji razmatra najvažnije zahteve i funkcionalnosti "pametne" električne mreže (engl. smart grid) u pogledu energetske efikasnosti, tehnologija neophodnih za implementaciju i očekivanih poboljšanja. Ukazuje na presudan značaj nanotehnologija za razvoj "pametne" mreže u bliskoj budućnosti.

Radovi u zbornicima sa međunarodnih konferencija štampani u celini ($M_{33} = 1$)

1. F. Darnell, V. Milutinovic, I. Branovic, M. Desivojevic, S. Ilic, V. Jovanovic, V. Jovicic, B. Milic, Dragana Milutinovic, S. Omorac, M. Savic, M. Simic, N. Uskokovic, Dj. Velickovic: Testing the E-business Infrastructure: Expanding into the Wireless/Mobile Environments, Proceedings of the 35th Annual IEEE Hawaii International Conference on System Sciences, pp. 3894 - 3898, 2002.
   http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=994524

   Preliminarni rezultati istraživanja objavljenih naknadno u časopisu Telecommunication Systems.

2. I. Branovic, R. Giorgi, A. Prete, Web-based training on computer architecture: The case for JCachesim, IEEE Workshop on Computer Architecture Education (WCAE-02), Anchorage, AK, USA, pp. 56-60, 2002. (citiran 15 puta)

   Opis razvijenog simulatora keš memorije procesora i prednosti njegovog korišćenja u nastavi predmeta Arhitektura računara.

3. I. Branovic, R. Giorgi, E. Martinelli, Memory performance of public-key cryptography methods in mobile environments, ACM SIGARCH Workshop on MEmory performance: DEaling with Applications, systems and architecture (MEDEA-03), New Orleans, LA, USA, pp. 24-31, 2003. (citiran 13 puta)

   Opis razvijenih test programa za šifrovanje eliptičkim krivama i njihovih performansi u pogledu zauzeća memorije u "embedded" uređajima. Uporedna analiza razvijenog testa sa drugim sličnim test programima.

4. I. Branovic, R. Giorgi, E. Martinelli, WebMIPS: A new web-based MIPS simulation environment for computer architecture education, Proceedings of the 2004 workshop on Computer architecture education, Munich, Germany, pp. 93-98, 2004. (citiran 34 puta)
   http://dl.acm.org/citation.cfm?id=1275596

   Opis razvijenog Web simulatora MIPS procesora i prednosti njegovog korišćenja u nastavi predmeta Arhitektura računara.

5. S. Bartolini, I. Branovic, R. Giorgi, E. Martinelli, A performance evaluation of ARM ISA extension for elliptic curve cryptography over binary finite fields, IEEE 16th Symposium on Computer Architecture and High Performance Computing, Foz do Iguacu, Brazil, pp. 238 - 245, 2004. (citiran 23 puta)
   http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1364759

   Preliminarni rezultati profiliranja izvršavanja metoda za šifrovanje eliptičkim krivama na "embedded" procesoru XScale i analiza mogućih dodataka skupu instrukcija, kasnije prošireni i objavljeni u časopisu IEEE Trsansactions on Computers.

6. S. Adamović, I. Branović, D. Živković, V. Tomašević, M. Milosavljević, Teaching interactive cryptography: the case for CrypTool, XLVI International Scientific Conference on Information, Communication and Energy Systems and Technologies - ICEST 2011, Niš, Srbija, pp. 1022 - 1024, 2011. (citiran 3 puta)
   http://www.icestconf.org/images/proceedings/icest_2011_03.pdf

   Opisuje pozitivna iskustva korišćenja alata CrypTool u nastavi predmeta Kriptografija.

7. I. Branović, S. Vesković, S. Mladenović, S. Milinković, S. Janković, SOA Architecture for Complying with EU Railway Timetable Data Exchange Format, TELSIKS'11 – 10th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, Niš, Serbia, pp. 630-631, 2011.
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6143191

   Implementacija Web servisa razvijenih za potrebe razmenjivanja reda vožnje u formatu koji propisuju EU standardi.

8. Z. Kostić, A. Jevremović, I. Branović, D. Marković, R. Popović, Dynamic Composition of Curriculum for Computer Science Courses, The Seventh International Conference on Internet and Web Applications and Services, Stuttgart, Germany, pp. 238 - 243, ISBN: 978-1-61208-200-4, 2012.
http://www.thinkmind.org/download.php?articleid=iciw_2012_8_30_20176

   Opis razvijene inovativne platforme za projektovanje kurikuluma predmeta, automatsko ocenjivanje i praćenje napretka studenta u virtuelnom okruženju.

9. M. Živković, I. Branović, D. Marković, R. Popović, Energy efficient security architecture for wireless sensor networks, Telecommunications Forum (TELFOR), Srbija, Beograd, pp. 1524 - 1527, ISBN 978-1-4673-2983-5, 2012.
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6419510

   Preliminarni rezultati istraživanja objavljenih naknadno u časopisu Telecommunication Systems.

10. M. Živković, I. Branović, D. Marković, R. Popović, Energy Efficient Security Architecture for Wireless Sensor Networks, Telecommunications Forum (TELFOR), Srbija, Beograd, pp. 1524 - 1527, 2012.
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6419510

    Pogled na potrošnju energije u bežičnim senzorskim mrežama i predlog klasterisane platforme koja bi koristila šifrovanje eliptičkim krivama čime bi se poboljšala njihova energetska efikasnost.

11. I. Branović, D. Marković, R. Popović, V. Tomasević, D. Živković, Development of modular virtual lab for introductory computing courses, IEEE Global Engineering Education Conference (EDUCON), Berlin, Germany, pp. 1027-1031, 2013.
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6530234

    Opisuje modularne virtuelne laboratorije razvijene za različite predmete informatike i računarstva i njihove prednosti u nastavi.

12. T. Živković, M. Živković, A. Khalifa, I. Branović, R. Popović, 3D Virtual laboratory for Wireless Sensor Networks, Telecommunications Forum (TELFOR), Srbija, Beograd, pp. 967 – 970, ISBN: 978-1-4799-1420-3/13, 2013.
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6716392

    Opisuje integraciju virtuelne laboratorije za bežične senzorske mreže u #D okruženje za učenje.

13. A. Khalifa, M. Živković, I. Branović, R. Popović, Internationalized approach to wireless networks simulation, Telecommunications Forum (TELFOR), Srbija, Beograd, pp. 869 – 872, ISBN 978-1-4799-1420-3/13, 2013.
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6716368

    Opisuje pozitivne efekte integracije simulatora za bežične senzorske mreže u višejezično 3D okruženje i organizovane sesije grupnog učenja koje su pomogle stranim studentima da prevaziđu jezičku barijeru.

14. I. Branovic, R. Giorgi, N. Jovanovic, R.Popovic, M.Zivkovic, B.Nikolic, Integration of simulators in virtual 3D computer science classroom, EDUCON, Istanbul, Turkey, pp. 1164 - 1167, 2013.
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7096837

    Opisuje pozitivne efekte integracije različitih simulatora razvijenih za računarske predmete (osnovi računarske tehnike, arhitektura računara, operativni sistemi, bežične mreže) u 3D virtuelno okruženje za učenje.

15. S. Janković, S. Mladenović, M. Vasiljević, I. Branović, S. Vesković, A Methodology of Developing Interoperable Electronic Business in the Transport Sector, Proceedings of XLVIII International Scientific Conference on Information, Communication and Energy Systems and Technologies - ICEST 2013, pp 515-518, Ohrid, Macedonia, 2013.
http://www.icestconf.org/images/proceedings/icest_2013_02.pdf

    Opis tehnologije korišćene za postizanje interoperabilnosti različitih subjekata uključenih u transportni sektor. Razmatra tri načina integracije: preko podataka, servisa i portala.

16. S. Janković, Ž. Djordjević, I. Branovic, S. Rajilic, S. Vesković, Database to support optimization of rolling stock maintenance in Serbian railways, XVI Scientific-Expert Conference on Railways - RAILCON '14, Niš, Serbia, pp. 149-152, ISBN 978-86-6055-060-8, 2014.

    Opis baze podataka, senzora za praćenje i informacionog sistema razvijenog za potrebe praćenja i održavanja voznih sredstava železnice.

Radovi u zbornicima sa konferencija nacionalnog značaja
štampani u celini ($M_{63} = 0.5$)

1. S. Vesković, S. Mladenović, S. Milinković, I. Branović, K. Dimanoski, Simulacioni model saobraćaja vozova na jednokolosečnoj pruzi u funkciji kvaliteta usluge, III međunarodni simpozijum "Novi horizonti saobraćaja i komunikacija 2011", pp. 43-47, Doboj, Bosna i Hercegovina, ISBN 978-99955-36-28-2, 2011.

   Opis simulacionog modela za istraživanje kapaciteta jednokolosečne pruge razvijenog u cilju podrške pri donošenju odluka koje se tiču propusne moći i kvaliteta pruge.

2. K. Dimanoski, G. Stojić, S. Vesković, I. Branović, Model za determinisanje kvaliteta usluga u putničkom železničkom prevozu, III međunarodni simpozijum "Novi horizonti saobraćaja i komunikacija 2011", pp. 43-47, Doboj, Bosna i Hercegovina, ISBN 978-99955-36-28-2, 2011.

   Rezultati istraživanja zadovoljstva putnika uslugom u železničkom saobraćaju u cilju povećanja konkurentnosti i profita.

3. S. Janković, S. Mladenović, I. Branović, S. Milinković, Cloud computing u saobraćaju, III međunarodni simpozijum "Novi horizonti saobraćaja i komunikacija 2011", pp. 692-697, Doboj, Bosna i Hercegovina, ISBN 978-99955-36-28-2, 2011.

   Razmatra modele "hostovanja" saobraćajno-transportnih servisa u "oblaku", kao i modele pristupa tim servisima. Prepoznate su oblasti u kojima se mogu iskoristiti prednosti cloud computing tehnologije: deljenje informacija i servisa od javnog značaja, podizanje nivoa kvaliteta e-poslovanja između transportnih javnih preduzeća, unapređenje sistema za odnos sa korisnicima.

4. I. Branović, M. Vasiljević, S. Vesković, S. Mladenović, S. Janković, 3D virtual classroom for training of railway staff, IV Medjunarodni simpozijum: Novi Horizonti 2013, Doboj, Bosna i Hercegovina, pp. 212-217, ISBN 978-99955-36-45-9, 2013.

   Opisan je proces razvoja 3D virtuelne učionice za obuku i osposobljavanje za rad različitih kategorija radnika železničkih izvršnih službi kao što su mašinovođe, radnici saobraćajne, tehničkokolske i transportno-komercijalne službe.

5. M. Milosavljević, I. Branović, S. Vesković, S. Milinković, N.Vasiljević, Simulacioni model železničko – drumskog terminala u tehnologiji pokretnih autostrada, YU INFO 2013, Kopaonik, Srbija, 2013.

6. B. Mitrović, S. Milinković, I. Branović, S. Vesković, S. Aćimović, Simulacioni model železničko-drumskog kontejnerskog terminala, YU INFO 2013, Informaciono društvo Srbije, Kopaonik, Srbija, 2013.

7. M. Milosavljević, S. Milinković, S. Vesković, I. Branović, S. Aćimović, Analiza sistema Bg voza primenom simulacionog paketa OpenTrack, YU INFO 2014, Kopaonik, Srbija: Informaciono društvo Srbije, pp. 473-478, 2014.

8. B. Mitrović, S. Milinković, S. Vesković, I. Branović, Ž. Djordjević, Model za lokaciju mernih stanica na mreži Železnica Srbije, YU INFO 2014, Kopaonik, Srbija: Informaciono društvo Srbije, pp. 467-472, 2014.
https://www.yuinfo.org/zbornik_2014_WEB%20verzija.pdf

Doktorska disertacija ($M_{71} = 6$)

1. I. Branović. *Instruction Set Extensions for Elliptic Curve Cryptography over Binary Finite Fields*. Dipartimento di Ingegneria dell'Informazione, Universita' degli Studi di Siena, Italia, 2005.
http://phd.dii.unisi.it/people/alumni.php

Tehnička rešenja ($M_{85} = 2$)

1. S. Mladenović, S. Janković, S. Vesković, I. Branović, SerbCross - SQL Azure baza podataka: Serbian Railroad Crossings, 2011, realizovano u okviru projekta TR36012

   Originalna baza podataka čiji je osnovni zadatak da integriše sve grupe podataka relevantne u oblasti upravljanja bezbednošću saobraćaja na putno-pružnim prelazima. Ovaj zadatak rešen je integracijom postojećih baza podataka koje nadležni subjekti koriste za potrebe upravljanja bezbednošću drumskog i železničkog saobraćaja na putno-pružnim prelazima.

Rezime kvantitativne valorizacije radova: Na osnovu navedenih podataka, a prema *Pravilniku o postupku i načinu vrednovanja, i kvantitativnom iskazivanju naučnoistraživačkih rezultata istraživača* radovi kandidata se kvantitativno valorizuju na sledeći način:

kategorija	br. poena	br. radova	ukupno poena
M12	10	1	10
M14	4	2	8
M21	8	2	16
M23	3	3	9
M33	1	16	16
M52	1.5	2	3
M53	1	2	2
M71	6	1	6
M85	1	2	2
M63	0.5	8	4
ukupno		39	76

Propisani minimalni kriterijumi za sticanje zvanja **viši naučni saradnik** u oblasti prirodno–matematičkih i medicinskih nauka, kao i ostvareni poeni kandidata, sumirani su u sledećoj tabeli:

	Ukupno	$M_{10} + M_{20} + M_{31} + M_{32} + M_{33} + M_{41} + M_{42} + M_{51}$	$M_{11} + M_{12} + M_{21} + M_{22} + M_{23} + M_{24} + M_{31} + M_{32} + M_{41} + M_{42}$
potrebno	64		
ostvareno	76		

Kvalitativni pokazatelji naučnog doprinosa kandidata

1. Pokazatelji uspeha u naučnom radu

Irina Branović je među članovima naučnog i organizacionog odbora konferencije YuInfo. Recenzent je u više istaknutih međunarodnih časopisa (IEEE Transactions on VLSI Systems (2 recenzije), Journal on Embedded Systems (3 recenzije)).

2. Angažovanost u razvoju uslova za naučni rad, obrazovanju i formiranju naučnih kadrova

3. Organizacija naučnog rada

4. Kvalitet naučnih rezultata

Najznačajniji rezultati kandidata objavljeni su u vrhunskim međunarodnim časopisima (IEEE Transactions on Computers, IF=1.659, Renewable and Sustainable Energy Reviews, IF 5.901).

U vezi sa citiranošću rezultata dr Irine Branović u naučnoj literaturi, komisiji su stavljeni na uvid sledeći podaci (autocitati, kako samog kandidata, tako i njegovih koautora ne navode se). Videti takođe Google Scholar profil:
https://scholar.google.com/citations?hl=sr&user=tW8FkHUAAAAJ

1. rad I. Branovic, R. Giorgi, E. Martinelli, WebMIPS: A new web-based MIPS simulation environment for computer architecture education, Proceedings of the 2004 workshop on Computer architecture education, Munich, Germany, pp. 93-98, 2004.

   citira se u

   - Vollmar, Kenneth, and Pete Sanderson. "MARS: an education-oriented MIPS assembly language simulator." ACM SIGCSE Bulletin. Vol. 38. No. 1. ACM, 2006.

- Chen, Yu, and Hessam S. Sarjoughian. "A component-based simulator for MIPS32 processors." Simulation (2009).
- Sarjoughian, Hessam, Yu Chen, and Kevin Burger. "A component-based visual simulator for mips32 processors." Frontiers in Education Conference, 2008. FIE 2008. 38th Annual. IEEE, 2008.
- Vegdahl, Steven R. "MIPSPILOT: A compiler-oriented MIPS simulator." Journal of Computing Sciences in Colleges 24.2 (2008): 32-39.
- ElAarag, Hala. "A complete design of a RISC processor for pedagogical purposes." Journal of Computing Sciences in Colleges 25.2 (2009): 205-213.
- Black, Michael David, and Priyadarshini Komala. "A full system x86 simulator for teaching computer organization." Proceedings of the 42nd ACM technical symposium on Computer science education. ACM, 2011.
- Soares, Sandro Neves, and Flávio Rech Wagner. "Design space exploration of embedded processors in computer architecture education using t&d-bench." Frontiers in Education Conference, 36th Annual. IEEE, 2006.
- Soares, Sandro Neves, and Flávio Rech Wagner. "T&D-Bench—Innovative Combined Support for Education and Research in Computer Architecture and Embedded Systems." Education, IEEE Transactions on 54.4 (2011): 675-682.
- Rodrigues, Rafael Porto, and CAPS MARTINS. "Ensino e aprendizado de pipeline de modo motivante e eficiente utilizando simuladores didáticos." WORKSHOP SOBRE EDUCAÇÃO EM ARQUITETURA DE COMPUTADORES (WEAC). 2008.
- Stojkovic, A., J. Djordjevic, and B. Nikolic. "WASP: a web-based simulator for an educational pipelined processor." International Journal of Electrical Engineering Education 44.3 (2007): 197-215.
- Fritz, David, Wira Mulia, and Sohum Sohoni. "The progressive learning platform." Workshop on Computer Architecture Education. 2011.
- Kabir, Md Tahsin, Mohammad Tahmid Bari, and Abul L. Haque. "ViSiMIPS: Visual simulator of MIPS32 pipelined processor." Computer Science & Education (ICCSE), 2011 6th International Conference on. IEEE, 2011.
- Sousa, BF de, et al. "WebSimple-MIPS: Simulador Web-based do Pipeline do MIPS." Workshop em Sistemas Computacionais de Alto Desempenho. 2008.
- Avelar, Cíntia P., et al. "MPDSim: Simulador didático do Pipeline do MIPS de 32 bits." Workshop sobre Educação em Arquitetura de Computadores WEAC. Vol. 2008. 2008.
- Azevedo, Hugo Costa, and Carlos Augusto Paiva da Silva Martins. "SIM-MIPS&HM-Simulador Didático do Nıvel ISA do MIPS e de Hierarquia de Memória." (2007): 1-4.

- Sohoni, Sohum, David Fritz, and Wira Mulia. "Transforming a microprocessors course through the progressive learning platform." ASEE Midwest Section, Russelville, AR (2011).
- Casillo, Leonardo Augusto, and Ivan Saraiva Silva. "Adapting a low complexity datapath to MIPS-1." Programmable Logic (SPL), 2012 VIII Southern Conference on. IEEE, 2012.
- Black, Michael, and Nathaniel Waggoner. "Emumaker86: a hardware simulator for teaching CPU design." Proceeding of the 44th ACM technical symposium on Computer science education. ACM, 2013.
- Alnoukari, Mouhib, Moutasem Shafaamry, and Kinaz Aytouni. "Simulation for Computer Sciences Education." Communications of the ACS 6.1 (2013): 49-54.
- Calvo Valdés, Francisco Alejandro, José Félix Roldán Ramírez, and Alfonso San Miguel Sánchez. "Simulador del procesador MIPS sobre el formalismo DEVS." (2010).
- Cosendey, Michael Martins, Rafael Henrique Brasil, and Carlos A. Paiva da Silva Martins. "SIPPIS MIPS: Um Novo Simulador de Pipeline do MIPS 32 bits para Auxílo à Educação em Arquitetura de Computadores."
- Valdés, Francisco Alejandro Calvo, et al. "Simulador del procesador MIPS sobre el formalismo DEVS."
- Sanderson, Pete, and Kenneth Vollmar. "MARS: An Education-Oriented MIPS Assembly Language Simulator." (2007): 239.
- Borth, Marcelo Rafael, and Aldo Sergio de Oliveira. "ALBOR: um simulador didático para auxiliar no ensino e aprendizagem de instruções Assembly." ForScience 2.1 (2014): 1-16.
- Rivas Pérez, Manuel, et al. "Diseño e implementación de un simulador software basado en el procesador MIPS32." (2015).
- García, Andrés Ortiz, Julio Ortega Lopera, and Alberto Prieto Espinosa. "Departamento de Arquitectura y Tecnología de Computadores ETS Ingenieria Informática y de Telecomunicación Universidad de Granada."
- Freitas, Alison RP, et al. "Arquitetura MIPS: desenvolvimento de um simulador." ANAIS do 9º. FÓRUM DE INFORMÁTICA E TECNOLOGIA DE MARINGÁ: 44.
- Torres, André LL, and Alisson V. Brito. "Extensão do Ptolemy para o ensino de Organização e Arquitetura de Computadores." Workshop sobre Educação em Arquitetura de Computadores.
- Silva, Gabriel Costa, and Rafael Cassolato de Meneses. "Um Ambiente Computacional de Apoio à Aprendizagem de Instruções Assembly."

- Araujo, Marcio Roberto Dias, et al. "MIPS X-Ray: A MARS Simulator Plug-in for Teaching Computer Architecture." International Journal of Recent Contributions from Engineering, Science & IT (iJES) 2.2 (2014): pp-36.
- García, Andrés Ortiz, and Julio Ortega Lopera. "Alternativas de externalización para la interfaz de red. Análisis y optimización mediante simulación de sistema completo."
- Mikki, Mohammad A., and Mohammed R. El-Khoudary. "Design of a Microsoft Version of MIPS Microprocessor Simulator."
- Foleiss, Juliano H., Valeria D. Feltrim, and Ronaldo AL Gonçalves. "SASM: uma ferramenta para o ensino do processo de montagem e de conjunto de instruções CISC."
- Nova, Bruno, Joao C. Ferreira, and António Araújo. "Tool to support computer architecture teaching and learning." Engineering Education (CISPEE), 2013 1st International Conference of the Portuguese Society for. IEEE, 2013.

2. rad I. Branovic, R. Giorgi, E. Martinelli, Memory performance of public-key cryptography methods in mobile environments, ACM SIGARCH Workshop on MEmory performance: DEaling with Applications, systems and architecture (MEDEA-03), New Orleans, LA, USA, pp. 24-31, 2003.

   citira se u

   - Rifa-Pous, Helena, and Jordi Herrera-Joancomartí. "Computational and energy costs of cryptographic algorithms on handheld devices." Future Internet 3.1 (2011): 31-48.
   - Ugus, Osman, et al. "Optimized implementation of elliptic curve based additive homomorphic encryption for wireless sensor networks." arXiv preprint arXiv:0903.3900 (2009).
   - Ugus, Osman, Alban Hessler, and Dirk Westhoff. "Performance of additive homomorphic EC-Elgamal encryption for TinyPEDS." 6. Fachgespräch Sensornetzwerke (2007): 55.
   - Alia, Mohammad Ahmad, and Azman Samsudin. "A New Digital Signature Scheme Based on Mandelbrot and Julia Fractal Sets." American Journal of Applied Sciences 4.11 (2007): 850-858.
   - Alia, Mohammad Ahmad, and Azman Samsudin. "New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets." International Journal of Computer Science and Network Security (IJCSNS) 7.2 (2007): 302-307.
   - Ugus, Osman, I. Huss, and D. Laue. "Asymmetric homomorphic encryption transformation for securing distributed data storage in wireless sensor networks." Technische Universit" at Darmstadt-in Cooperation with NEC Europe Ltd., Heidelberg, Darmstadt (2007).

- Alia, Mohammad Ahmad, and Azman Samsudin. "A New Public-Key Cryptosystem Based On Mandelbrot And Julia Fractal Sets." Asian journal of Information technology 6.5 (2007): 567-575.
- Alia, Mohammad Ahmad, and Azman Bin Samsudin. "A New Digital Signature Scheme Based on Mandelbrot and Julia Fractal Sets." American Journal of Applied Sciences 4.11 (2007): 848-856.
- Al-Anie, Hayam K., Mohammad A. Alia, and Adnan A. Hnaif. "EVoting PROTOCOL BASED ON PUBLIC-KEY CRYPTOGRAPHY." International Journal Of Network Security & Its Applications 3.4 (2011): 87-98.
- Alia, Mohammad A., Abdelfatah Aref Tamimi, and Omaima NA AL-Allaf. "Cryptography Based Authentication Methods." Proceedings of the World Congress on Engineering and Computer Science. Vol. 1. 2014.
- Herrera Joancomartí, Jordi, and Helena Rifà Pous. "Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices." (2011).
- Alia, Mohammad Ahmad. "Cryptosystems Based on Chaos Theory." Chaos, Complexity and Leadership 2013. Springer International Publishing, 2015. 129-145.
- Rashwan, Abdulmonem M., Abd-Elhamid M. Taha, and Hossam S. Hassanein. "Characterizing the Performance of Security Functions in Mobile Computing Systems." Internet of Things Journal, IEEE 1.5 (2014): 399-413.

3. rad D. S. Marković, D. Živković, I. Branović, R. Popović, D. Cvetković, Smart Power Grid and Cloud Computing, Renewable and Sustainable Energy Reviews, 24: 566–577, 2013.

   citira se u

   - Fadaeenejad, M., et al. "The present and future of smart power grid in developing countries." Renewable and Sustainable Energy Reviews 29 (2014): 828-834.
   - Reddy, K. S., et al. "A review of Integration, Control, Communication and Metering (ICCM) of renewable energy based smart grid." Renewable and Sustainable Energy Reviews 38 (2014): 180-192.
   - Yigit, Melike, V. Cagri Gungor, and Selcuk Baktir. "Cloud computing for smart grid applications." Computer Networks 70 (2014): 312-329.
   - Chofreh, Abdoulmohammad Gholamzadeh, et al. "Sustainable enterprise resource planning: imperatives and research directions." Journal of Cleaner Production 71 (2014): 139-147.
   - Mahmood, Anzar, Nadeem Javaid, and Sohail Razzaq. "A review of wireless communications for smart grid." Renewable and Sustainable Energy Reviews 41 (2015): 248-260.

- Kiciński, J. "Do we have a chance for small-scale energy generation? The examples of technologies and devices for distributed energy systems in micro & small scale in Poland." Bulletin of the Polish Academy of Sciences: Technical Sciences 61.4 (2013): 749-756.
- Chou, Jui-Sheng, and Abdi Suryadinata Telaga. "Real-time detection of anomalous power consumption." Renewable and Sustainable Energy Reviews 33 (2014): 400-411.
- Powell, Kody Merlin. "Dynamic optimization of energy systems with thermal energy storage." (2013).
- Fons Gomez, Fernando Jose. Cloud Computing: caracterización de los impactos positivos obtenidos por la utilización del modelo Cloud Computing por las pymes, basado en la tipología de Modelos de Negocio de este tipo de empresas. Diss. 2014.
- Patti, Edoardo, et al. "Distributed Software Infrastructure for General Purpose Services in Smart Grid."
- Diamantoulakis, Panagiotis D., Vasileios M. Kapinas, and George K. Karagiannidis. "Big Data Research." (2015).
- Zhenxing, Zhao, et al. "Design and Implementation of Energy Hub for Smart Grid." Intelligent Systems Design and Engineering Applications, 2013 Fourth International Conference on. IEEE, 2013.
- Colak, Ilhami, et al. "A survey on the contributions of power electronics to smart grid systems." Renewable and Sustainable Energy Reviews 47 (2015): 562-579.
- Amaro, Nuno, et al. "Combined Operation of an Unified Power Quality Conditioner and a Superconducting Magnetic Energy Storage System for Power Quality Improvement." Technological Innovation for Cloud-Based Engineering Systems. Springer International Publishing, 2015. 374-382.
- Khan, Zeeshan Ali, and Yasir Faheem. "Cognitive radio sensor networks: Smart communication for smart grids—A case study of Pakistan." Renewable and Sustainable Energy Reviews 40 (2014): 463-474.
- Song, Xin, et al. "A Massive Sensor Data Streams Multi-dimensional Analysis Strategy Using Progressive Logarithmic Tilted Time Frame for Cloud-Based Monitoring Application." Advances in Neural Networks–ISNN 2014. Springer International Publishing, 2014. 550-557.
- Nair, Rajeev Thankappan, and Ashok Sankar. "Dynamic pricing based on a cloud computing framework to support the integration of renewable energy sources." The Journal of Engineering 1.1 (2014).
- Garrab, Asma, Ammar Bouallegue, and Ridha Bouallegue. "Multi-Agent modeling of a meters network used in Smart Grid." Computer Applications and Information Systems (WCCAIS), 2014 World Congress on. IEEE, 2014.

- Pei, Wei, et al. "Design and Implementation of Energy Management System for Energy Hub in Smart Grid." Information Technology Journal 12.18 (2013): 4797-4804.
- Al Abria, Dawood, et al. "Smart Grid." (2015).
- Califano, Anthony, Ersin Dincelli, and Sanjay Goel. "Using Features of Cloud Computing to Defend Smart Grid against DDoS Attacks." 10th Annual Symposium on Information Assurance (ASIA'15). 2015.
- Macedo, Maria NQ, et al. "Typification of load curves for DSM in Brazil for a smart grid environment." International Journal of Electrical Power & Energy Systems 67 (2015): 216-221.
- Roppestad, Robert, Per-Gunnar Fyhn, and Ricardo Colomo-Palacios. "A test bed for smart energy education in the field of computer engineering." Proceedings of the Second International Conference on Technological Ecosystems for Enhancing Multiculturality. ACM, 2014.
- Guerrero, Juan I., et al. "Improving Knowledge-Based Systems with statistical techniques, text mining, and neural networks for non-technical loss detection." Knowledge-Based Systems 71 (2014): 376-388.
- Rajeev, T., and S. Ashok. "Dynamic load-shifting program based on a cloud computing framework to support the integration of renewable energy sources." Applied Energy 146 (2015): 141-149.
- Li, Jing, et al. "Computing Mode Study of Large-Scale Power Grid Online Analysis Software Based on Cloud Computing Technology." Applied Mechanics and Materials. Vol. 427. 2013.
- Huang, Qi, et al. "Data Management in Smart Grid." Innovative Testing and Measurement Solutions for Smart Grid: 183-210.
- Zhou, Kaile, and Shanlin Yang. "A framework of service-oriented operation model of China's power system." Renewable and Sustainable Energy Reviews 50 (2015): 719-725.
- Kiciński, Jan, and Grzegorz Żywica. "Distributed Cogeneration. Civic Power Engineering. New Ideas." Steam Microturbines in Distributed Cogeneration. Springer International Publishing, 2014. 1-16.
- Diamantoulakis, Panagiotis D., Vasileios M. Kapinas, and George K. Karagiannidis. "Big Data Analytics for Dynamic Energy Management in Smart Grids." Big Data Research (2015).

4. rad S. Bartolini, I. Branovic, R. Giorgi, E. Martinelli, A performance evaluation of ARM ISA extension for elliptic curve cryptography over binary finite fields, IEEE 16th Symposium on Computer Architecture and High Performance Computing, Foz do Iguacu, Brazil, pp. 238 - 245, 2004.

   citira se u

- Regazzoni, Francesco, et al. "A design flow and evaluation framework for DPA-resistant instruction set extensions." Cryptographic Hardware and Embedded Systems-CHES 2009. Springer Berlin Heidelberg, 2009. 205-219.
- Grabher, Philipp, Johann Großschädl, and Dan Page. "Light-weight instruction set extensions for bit-sliced cryptography." Cryptographic Hardware and Embedded Systems–CHES 2008. Springer Berlin Heidelberg, 2008. 331-345.
- Elbirt, Adam J. "Fast and efficient implementation of AES via instruction set extensions." Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on. Vol. 1. IEEE, 2007.
- Gueneysu, Tim, Christof Paar, and Jan Pelzl. "Attacking elliptic curve cryptosystems with special-purpose hardware." Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays. ACM, 2007.
- Melia, Sean O., and Adam J. Elbirt. "Enhancing the performance of symmetric-key cryptography via instruction set extensions." Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 18.11 (2010): 1505-1518.
- Elbirt, Adam J. "Accelerated AES implementations via generalized instruction set extensions." Journal of Computer Security 16.3 (2008): 265-288.
- Jachimiec, Nathan P., Fernando Martinez-Vallina, and Jafar Saniie. "Acceleration of finite field arithmetic algorithms in embedded processing platforms utilizing instruction set extensions." Electro/Information Technology, 2007 IEEE International Conference on. IEEE, 2007.
- Jachimie, Nathan, Fernando Martinez-Vallin, and Jafar Saniie. "CReconfigurable finite field instruction set architecture." Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays. ACM, 2007.
- Tanimura, Kazuyuki, et al. "Unified Dual-Radix Architecture for Scalable Montgomery Multiplications in GF (P) and GF (2 n)." IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences 92.9 (2009): 2304-2317.
- Gora, Michael, Eric Simpson, and Patrick Schaumont. "Intellectual Property Protection for Embedded Sensor Nodes." Embedded Computer Systems: Architectures, Modeling, and Simulation. Springer Berlin Heidelberg, 2008. 289-298.
- Smari, Waleed W., Luca Spalazzi, and Yacine Zemali. "Editorial: Recent developments in high performance computing and security: An editorial." Future Generation Computer Systems 29.3 (2013): 782-787.
- Joshi, Pallavi. Towards Faster Cryptography. Diss. Indian Institute of Technology Kharagpur, 2006.

- Gora, Michael Arthur. "Securing Software Intellectual Property on Commodity and Legacy Embedded Systems." (2010).
- Kim, Dae-Hwan. "AMEX: Extending Addressing Mode of 16-bit Thumb Instruction Set Architecture." Journal of The Korea Society of Computer and Information 17.11 (2012): 1-10.

5. rad I. Branovic, R Giorgi, E Martinelli, A workload characterization of elliptic curve cryptography methods in embedded environments, ACM SIGARCH Computer Architecture News, 32 (3): 27-34, 2004.

   citira se u

   - Durlanik, Aytunc, and Ibrahim Sogukpinar. "SIP authentication scheme using ECDH." World Enformatika Society Transations on Engineering Computing and Technology 8 (2005): 350-353.
   - Yoon, Eun-Jun, et al. "A secure and efficient SIP authentication scheme for converged VoIP networks." Computer Communications 33.14 (2010): 1674-1681.
   - Milenković, Milena, Aleksandar Milenković, and Emil Jovanov. "Hardware support for code integrity in embedded processors." Proceedings of the 2005 international conference on Compilers, architectures and synthesis for embedded systems. ACM, 2005.
   - Yoon, Eun-Jun, et al. "Robust mutual authentication with a key agreement scheme for the session initiation protocol." IETE Technical Review 27.3 (2010): 203-213.
   - Ahmad, Tohari, Jiankun Hu, and Song Han. "An efficient mobile voting system security scheme based on elliptic curve cryptography." Network and System Security, 2009. NSS'09. Third International Conference on. IEEE, 2009.
   - Milenkovic, Milena. Architectures for run-time verification of code integrity. Diss. The University of Alabama in Huntsville, 2005.
   - Rogers, Austin, Milena Milenkovic, and Aleksandar Milenkovic. "A low overhead hardware technique for software integrity and confidentiality." Computer Design, 2007. ICCD 2007. 25th International Conference on. IEEE, 2007.
   - Rogers, Austin, and Aleksandar Milenković. "Security extensions for integrity and confidentiality in embedded processors." Microprocessors and Microsystems 33.5 (2009): 398-414.
   - Milenkovic, Aleksandar, Milena Milenkovic, and Emil Jovanov. "An efficient runtime instruction block verification for secure embedded systems." Journal of Embedded Computing 2.1 (2006): 57.
   - Puzović, Nikola, et al. "A multi-pronged approach to benchmark characterization." Cluster Computing Workshops and Posters (CLUSTER WORKSHOPS), 2010 IEEE International Conference on. IEEE, 2010.

- Rogers, Austin. Designing Cost-effective Secure Processors for Embedded Systems: Principles, Challenges, and Architectural Solutions. Diss. The University of Alabama in Huntsville, 2010.
- Zhang, Liping, Shanyu Tang, and Zhihua Cai. "Robust and efficient password authenticated key agreement with user anonymity for session initiation protocol-based communications." Communications, IET 8.1 (2014): 83-91.
- de Oliveira, Augusto Born, Ahmad Saif Ur Rehman, and Sebastian Fischmeister. "mTags: augmenting microkernel messages with lightweight metadata." ACM SIGOPS Operating Systems Review 46.2 (2012): 67-79.
- Yoon, Eun-Jun, and Kee-Young Yoo. "Robust biometric-based three-party authenticated key establishment protocols." International Journal of Computer Mathematics 88.6 (2011): 1144-1157.
- Karaoğlan, Duygu, and Albert Levi. "A survey on the development of security mechanisms for body area networks." The Computer Journal 57.10 (2014): 1484-1512.
- Rogers, Austin. Low Overhead Hardware Techniques for Software and Data Integrity and Confidentiality in Embedded Systems. Diss. The University of Alabama in Huntsville, 2007.
- Gora, Michael, Eric Simpson, and Patrick Schaumont. "Intellectual Property Protection for Embedded Sensor Nodes." Embedded Computer Systems: Architectures, Modeling, and Simulation. Springer Berlin Heidelberg, 2008. 289-298.
- Saif Ur Rehman, Ahmad. "Tags: Augmenting Microkernel Messages with Lightweight Metadata." (2012).
- Quirino, Gustavo S., Edward David Moreno, and Leila BC Matos. "Performance Evaluation of Asymmetric Encryption Algorithms in embedded platforms used in WSN." Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2013.
- Gora, Michael Arthur. "Securing Software Intellectual Property on Commodity and Legacy Embedded Systems." (2010).

6. rad S. Bartolini, I. Branović, R. Giorgi, E. Martinelli, Effects of Instruction-set Extensions on an Embedded Processor: a Case Study on Elliptic Curve Cryptography over GF(2m), IEEE Transansactions on Computers, 57(5):672–685, 2008.

   citira se u

   - Oliveira, Leonardo B., et al. "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks." Computer Communications 34.3 (2011): 485-493.

- Tergino, Christian Sean. "Efficient binary field multiplication on a VLIW DSP." (2009).
- Kobayashi, Kaoru, Naofumi Takagi, and Kazuyoshi Takagi. "Fast inversion algorithm in GF (2m) suitable for implementation with a polynomial multiply instruction on GF (2)." IET computers & digital techniques 6.3 (2012): 180-185.
- Erdem, Serdar Süer. "Fast software multiplication in F2 [x] for embedded processors." Turkish Journal of Electrical Engineering & Computer Sciences 20.4 (2012).
- Sakthivel, A., and R. Nedunchezhian. "Decreasing point multiplication over ECC (Z p) using tree computations." Computing, Communication and Applications (ICCCA), 2012 International Conference on. IEEE, 2012.
- Sakthivel, A., and R. Nedunchezhian. "Optimizing point Doubling Operations in ECC Zp." International Journal of Computer Applications 41.6 (2012).
- Sakthivel, Arumugam, and Dr R. Nedunchezhian. "Analyzing the Point Multiplication Operation of Elliptic Curve Cryptosystem over Prime Field for Parallel Processing." International Arab Jounal of Information Technology 11.4 (2014): 1-7.
- Keramidas, Georgios, et al. "Embedded reconfigurable computing: the ERA approach." Industrial Informatics (INDIN), 2013 11th IEEE International Conference on. IEEE, 2013.
- Hamilton, Mark. "Cryptographic coprocessors for embedded systems." (2014).
- Winson, Ninh. "Performance Comparison of Projective Elliptic-curve Point Multiplication in 64-bit x86 Runtime Environment." (2014).

7. rad S. Adamović, I. Branović, D. Živković, V. Tomašević, M. Milosavljević, Teaching interactive cryptography: the case for CrypTool, XLVI International Scientific Conference on Information, Communication and Energy Systems and Technologies - ICEST 2011, Niš, Srbija, 2011.

   citira se u

   - El Farra, Ahmad, and Edmond Zahedi. "Interactive educational tool for teaching a simple cipher." Biometrics and Security Technologies (ISBAST), 2014 International Symposium on. IEEE, 2014.
   - Katz, Frank H. "A Comparison of Different Methods of Instruction in Cryptography." (2014).

Kako se iz navedenih podataka može zaključiti, sedam publikacija dr Irine Branović citirano je ukupno više od 120 puta u svetskoj naučnoj literaturi. Rezultati Irine Branović citirani su u raznorodnim publikacijama, počev od doktorskih teza i istraživačkih izveštaja sa renomiranih svetskih univerziteta, preko saopštenja na međunarodnim skupovima, pa do radova u vrhunskim međunarodnim časopisima (kao što su IEEE Transactions on Education (čiji je impakt faktor 0.842), Renewable and Sustainable Energy Reviews (IF=5.901), Computer Networks (IF=1.256), Journal of Cleaner Production (IF=3.844), Knowledge-Based Systems (IF=2.947), Applied Energy (IF=5.612), IEEE Transactions on VLSI Systems (IF=1.356), Future Generation Computer Systems (IF=2.786), Computer Communications (IF= 1.695) i dr.), i poglavlja u monografijama renomiranih svetskih izdavača (Springer).

Iako dr Irina Branović nema samostalnih radova, ona je pokretački faktor u istraživačkim grupama sa kojima sarađuje. Njeni koautori su renomirani svetski eksperti koji su direktno uticali na njen razvoj i afirmaciju i/ili kolege istraživači. Svi test primeri, razvijeni simulatori i drugi rezultati dostupni su svetskoj istraživačkoj javnosti preko Interneta, na šta upućuju linkovi u odgovarajućim radovima. Iskustvo stečeno na obrazovanju u inostranstvu koje kandidat ima doprinosi proširenju međunarodne saradnje kako samog kandidata, tako i njene matične institucije. Sve to potvrđuju i njeni koautori u svojim izjavama.

Značaj rezultata koje je dr Branović ostvarila u svom dosadašnjem istraživačkom radu višestruk je. Razvijeni simulatori i test softver za utvrđivanje efikasnosti metoda za šifrovanje eliptičkim krivama opšteprihvaćeni su i korišćeni u novijoj literaturi o čemu svedoče brojni citati referentnih radova. Novi problemi i metode koje je predočila u svojim radovima, razmatraju se kako u svetu, tako i u našim institucijama.

Zaključak

Iz navedenih podataka vidi se da dr Irina Branović aktivno i uspešno učestvuje u naučno–istraživačkom radu u oblasti računarstva. Koautor je više radova objavljenih u međunarodnim časopisima i saopštenih kako na međunarodnim, tako i na domaćim konferencijama. Mnogi od njih su višestruko citirani u stranoj naučnoj literaturi. Aktivno učestvuje i u drugim stručnim aktivnostima Matematičkog instituta.

Na osnovu spiska objavljenih radova i njihove valorizacije na osnovu *Pravilnika o postupku i načinu vrednovanja, i kvantitativnom iskazivanju naučnoistraživačkih rezultata istraživača* može se zaključiti da kandidat dr Irina Branović ispunjava i kvantitativne i kvalitativne kriterijume za izbor u zvanje viši naučni saradnik.

Imajući u vidu navedene činjenice, sa zadovoljstvom predlažemo Naučnom veću Matematičkog instituta SANU da dr Irinu Branović Balović izabere u naučno zvanje **viši naučni saradnik** za oblast računarstvo.

U Beogradu
30. jun 2015.

Članovi komisije

dr Tatjana Davidović,
viši naučni saradnik MI SANU

prof.dr Miomir Stanković,
redovni profesor Fakulteta zaštite na radu

dr Slobodan Simić,
naučni savetnik MI SANU