Synthesis
International Scientific Conference of IT and Business-Related Research

DIZAJN GENERATORA ISTINSKI SLUČAJNIH BROJEVA KORIŠĆENJEM BUKE U ŽIVOTNOJ SREDINI

DESIGN OF A TRUE RANDOM NUMBER GENERATOR USING ENVIRONMENTAL NOISE

Slaviša Nikolić, Dejan Uljarević
Departman za poslediplomske studije, Univerzitet Singidunum, Danijelova 32, Beograd, Srbija

Apstrakt:
U ovom radu je prikazan metod dobijanja istinski slučajnih bitova korišćenjem hardvera zvučne kartice računara, na čiji se audio ulaz dovodi slučajni signal buke u životnoj sredini a za post-procesiranje se koristi nov postupak post-procesiranja tzv. „miksovanje bita u koracima i XOR-ovanje susednih bita" (MiBiS&XOR). Predstavljenim postupkom destilacije se na jednostavan i efikasan način susedni ulazni bitovi, koji su u određenoj korelaciji, razdvajaju i udaljuju jedni od drugih, čime se smanjuje autokorelacija a zatim se u novodobijenom nizu susedni bitovi XOR-uju čime se povećava entropija i smanjuje odstupanje izlaznog bitskog niza. Eksperimentalna statistička testiranja slučajnosti vršena na nizovima bitova dobijenim kao rezultat predložene metode potvrđuju kvalitet izlaza generatora istinski slučajnih brojeva (TRNG).

Ključne reči:
buka u životnoj sredini, zvučna kartica, entropija, statistički testovi.

Abstract:
This paper presents a method of obtaining true random bits using hardware of a computer sound card, with a random environmental noise signal being brought to its audio input by means of a microphone. A new procedure of distributing bits is used for post-processing, which is also called "mixing bits in steps and XORing of adjacent bits" (MiBiS&XOR). The given distillation procedure enables separating and dividing correlated adjacent input bits in a simple and efficient way, thus reducing the total auto-correlation. In this new sequence,adjacent bits are then XORed, which increases entropy and reduces bias of the output bit sequence. Experimental statistical randomness tests performed on the sequences of bits obtained as a result of the proposed method, confirm the excellent quality of a true random number generator (TRNG) output.

Key words:
environmental noise, sound card, entropy, statistical tests.

1. UVOD

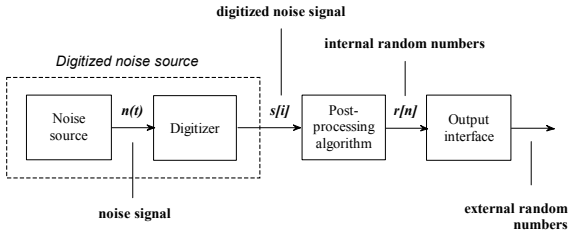
Slučajni brojevi su ključni sastojci čitavog niza oblasti, uključujući kriptografiju, simulacije, igre na sreću, uzorkovanje, donošenje odluka, medicinu i estetiku kao i umetnost. Najčešće korišćeni generatori slučajnih brojeva su generatori pseudo-slučajnih brojeva (PRNG). Generatori pseudo-slučajnih brojeva su ništa drugo nego matematičke formule koje proizvode determinističke, periodične nizove brojeva koje u potpunosti određuje početno odnosno inicijalno stanje koje se naziva SID (Gentle, 2004). Međutim, u nekim slučajevima generisanim vrednostima nedostaju jake statističke karakteristike. To su zahtevne situacije u kojima se PRNG generatori zamenjuju TRNG-ima, kao što su generisanje kriptografskih ključeva, generisanje lista kod igara na sreću ili statističke simulacije. TRNG-i se zasnivaju na nedeterminističkim izvorima kao što su audio šumovi (Morrison, 2001), radioaktivno raspadanje, termalni šumovi generisani od strane poluprovodnika, termalni šumovi kod otpornika, fotoelektrični efekti ili razni kvantni fenomeni (Konar & Biswas, 2005). Haotično ponašanje uzrokovano ovakvim pojavama može se iskoristiti kao izvor entropije u dizajnu TRNG-a.

Određivanje raspoložive entropije i njenih tačnih statističkih osobina kao i ispitivanje dugoročnih efekata koji mogu izazvati pogoršanje kvaliteta entropije izvora su sledeći važni zadaci kod određivanja dizajna TRNGa (Mankad & Pradhan, 2012). Međutim, iako su mnogobrojne aktivne monitoring tehnike za detekciju kvarova na raspolaganju, suptilnije greške je u praksi vrlo teško otkriti i predvideti.

Istinski slučajani brojevi se dobijaju iz istinski slučajnog bitskog niza u kome su bitovi nezavisni i nepristrasni. Pošto se slučajni brojevi koriste u različite svrhe, postavljaju se različiti zahtevi koji se odnose na kvalitet generisane sekvence. Na primer, kod aplikacija za simulacije obično je dovoljno da su ispunjeni uslovi nezavisnosti brojeva i identična distribucija. Međutim, u kriptografiji je jedan od glavnih zahteva nemogućnost pogađanja sledećeg broja u nizu. Kriptosistemi visokog stepena bezbednosti ne mogu se zamisliti bez TRNG-a koji predstavljaju fundamentalne delove takvih sistema osiguravajući svojim kvalitetom bezbednost ključa, a time i sigurnost celog sistema (Schindler & Killmann, 2002).

Rad TRNG-a se može podeliti u tri faze (Slika 1). Prva faza je generisanje digitalizovanog analognog signala (DAS), koji se dobijaju iz izvora kao što su npr. mikrokosmički procesi (tj. termalni šum poluprovodnika ili šum sačme kod Zener diode), kao i periodično digitalizovanje vremenski kontinualnog analognog signala izvora. Druga faza je generisanje internih (unutrašnjih) slučajnih brojeva, koji predstavljaju DAS slučajne brojeve nakon njihove post-obrade kako bi smanjili njihove slabosti raspodele. Treća faza je dobijanje tzv. spoljašnjih slučajnih brojeva i ona korespondira sa konačnim rezultatom algoritma za vađenje slučajnog broja. Ovaj pristup je usvojen 2001. godine od strane Nemačkog IT Bezbedonosno Sertifikacionog Tela (BSI) u njihovoj 31 AIS publikaciji.

E-mail: nikolic.slav@yahoo.com
DOI: 10.15308/Synthesis-2015-97-100



Slika 1. Princip rada TRNGa

U ovom radu se za dobijanje istinski slučajnih brojeva koristi zvučna kartica standardnog hardvera personalnih desktop računara ili novijih generacija lap topova , tableta ili mobilnih smart telefona, na koju se preko mikrofona dovodi slučajni signal buke životne sredine. Prikazano je i korišćenje nove metode post-procesiranja tzv. „miksovanje bitova u koracima a zatim XOR-ovanje susednih bitova", kojom se na inovativan način smanjuje autokorelacija a povećava ukupna entropija izlaznog bitskog niza. Statistički testovi slučajnosti, pre svega oni koji se odnose na entropiju i autokorelaciju, vršeni na nizu bitova dobijenih kao rezultat nove metode, potvrđuju kvalitet izlaza TRNG-a.

2. REZULTATI I DISKUSIJA

Kao fizički izvor slučajnosti u ovom radu se, u cilju dobijanja istinski slučajnih bitova, koristi šum buke životne sredine koje u gradovima ima u izobilju, vrlo često i iznad dozvoljenih granica. Posmatrani slučajevi buke bili su:

#1 Razgovori velikog broja pešaka u najprometnijoj pešačkoj ulici u gradu,
#2 Saobraćajna buka,
#3 Buka u prometnom podzemnom pešačkom prolazu,
#4 Buka na žurci, nastala kao proizvod bučnih razgovora velikog broja učesnika i muzike u pozadini i
#5 Miksovana buka (saobraćajna buka, konverzaciona buka velikog broja učesnika i multimedijalni zvuci)

Za dobijanje istinski slučajnih bitova koristila se zvučna kartica računara, na koju se preko mikrofona dovodi slučajni analogni signal buke. Kretanje, odnosno pomeranje raznih stvari, saobraćajna buka, razgovori većeg broja ljudi kao i sva ova buka zajedno, koja predstavlja buku životne sredine, stvara veliki broj zvučnih talasa različitih frekfencija, amplituda i faza, koji prolazeći kroz vazduh i odbijajuće se od objekata stvaraju u mikrofonu signal nepredvidljivih amplitudnih vrednosti. Analogni zvuk se u mikrofonu konvertuje u napon a onda nakon ADC-a u podatke u obliku bita. Gustina raspodele amplituda najveća je za vrednosti signala 0 i postepeno se smanjuje za vrednosti amplituda koje su različite od nule. Ovakva raspodela kod koje je verovatnoća pojavljivanja određenih vrednosi veća od verovatnoće pojavljivanja drugih vrednosti je nepoželjna jer samim tim vrednosti niza ne zadovoljavaju karakteristike slučajnosti. Kvalitetan niz slučajnih vrednosti mora imati ravnomernu odnosno uniformnu raspodelu vrednosti kako bi bili zadovoljeni osnovni kriterijumi slučajnosti kao što su nepredvidivost, nepristrasnost i nezavisnost jednih od drugih. Post-procesiranjem se u stvari vrši transformisanje digitalizovanih slučajnih vrednosti signala sa normalnom raspodelom u uniformno raspoređene slučajne vrednosti, čak i ako inicijalni signal ima značajne statističke nedostatke. Velikom brzinom odmereni, podaci odmeraka imaju nedozvoljeno visoka korelaciona svojstva. Ovo je očekivano jer se odmerava kontinualan i ponekad sporo promenljiv analogni signal. U ovom radu prikazan je novi postupak postprocesiranja MiBiS&XOR. Kao rezultat dobija se novi niz bitova kod koga je smanjena korelacija između bitova, smanjena sistemska greška, a povećana ukupna entropija bitskog niza.

U prvom koraku mikser prihvata prva dva dolazeća bita iz ADCa. U drugom koraku prihvata treći bit i smešta ga između njih. Ako bitove obeležimo brojevima po redosledu dolaska onda bi taj raspored u drugom koraku bio x1,x3,x2, pri čemu svako x predstavlja promenljivu koja može imati dve vrednosti [0,1]. Četvrti bit se zatim, u trećem koraku, smešta između prvog i trećeg a peti između trećeg i drugog. Sada je raspored bita x1,x4,x3,x5,x2. U četvrtom koraku se šesti bit smešta između 1 i 4, sedmi između 2 i 5, osmi između 4 i 3 a deveti između 5 i 3. Time se završava četvrti korak a dobijeni raspored je x1,x6,x4,x8,x3,x9,x5,x7,x2. Primenom istog postupka po završetku petog koraka dobija se sledeći raspored bita u ovim korakom nastalom nizu: x1,x10,x6,x12,x4,x14,x8,x16,x3,x17,x9,x15,x5,x13,x7,x11,x2. Sledeći koraci se ponavljaju na isti način sve dok se ne rasporede svi ulazni bitovi.

Ukupan broj bita niza dobijenog nakon primene određenog broja koraka iznosi

$$y_n=2^{n-1}+1 \quad (1)$$

gde je n broj koraka i $n = 1,2,3,...,\infty$.

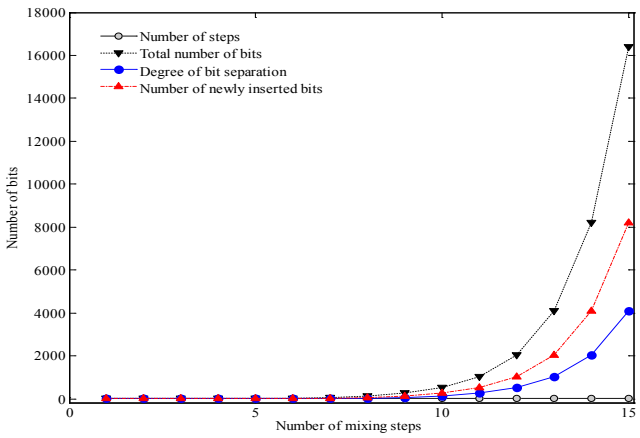
Ako je poznato koliko se bitova koristi za miksovanje može se izračunati koliko koraka mikser treba da napravi da bi se izmešali svi bitovi, pa je

$$n=log_2(y_n-1)+1 \quad (2)$$

Ukupan broj novoubačenih bita (u odnosu na niz iz prethodnog koraka) izračunava se po formuli:

$$m_n=2^{n-2} \quad (3)$$

Rastojanje ili razmak između uzastopnim rasporedom primljenih bita iz ADC-a, se u principu povećava povećanjem koraka miksovanja. Naime, dobijeni raspored bita posle trećeg koraka miksovanja je x1,x4,x3,x5,x2 pa najmanje rastojanje u redosledu prihvaćenih bita iznosi jedan. U četvrtom koraku je dobijeni raspored bita x1,x6,x4,x8,x3,x9,x5,x7,x2 pa stepen razdvajanja iznosi dva zato što se u nizu pojavljuju bitovi čije je najmanje rastojanje u rasporedu redosleda primljenih bita dva (x6,x4 i x5,x7) što praktično znači da postoje susedni bitovi u nizu koji su kao svaki drugi prihvaćeni iz ADCa. Vrednosti stepena razdvajanja bita u nizovima istinski slučajnih bita dobijenih metodom „miksovanja bita u koracima" eksponencijalno se povećavaju povećanjem koraka miksovanja kao što je prikazano na Sl. 2.



Slika 2. Graficki prikaz zavisnosti ukupnog broja bita, dobijenog razmaka izmedju bita i novoubačenih bita od broja koraka mešanja

DOI: 10.15308/Synthesis-2015-97-100

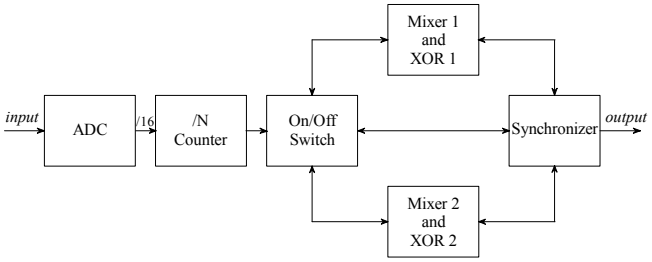
Matematička formula, kojom se izračunava stepen razdvajanja bita kod nizova slučajnih bita dobijenih metodom „miksovanja bita u koracima", posle n koraka miksovanja je

$$d_n = 2^{n-3} \quad (4)$$

gde je n broj koraka miksovanja i $n = 3,4,5,\ldots, \infty$.

Na kraju se, u izlaznom nizu iz miksera, XOR-uju svi susedni bitovi čime se dobija konačan niz istinski slučajnih bita.

Dobijanje slučajnih bita u realnom vremenu predstavljenom metodom moguće je izvesti i korišćenjem samo jednog miksera i XOR-a, međutim u ovom slučaju bi dolazni bitovi iz ADC-a, sve dok traje obrada prethodnih bita, bili nepovratno izgubljeni. Rešenje je pronađeno korišćenjem dva nezavisna miksera koji naizmenično rade (Sl. 3).



Slika 3. Proces dobijanja slučajnih bita korišćenjem dva miksera i dva XOR-a

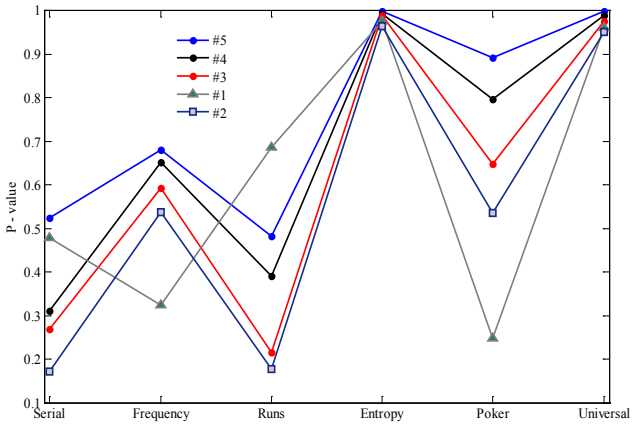
Naime, prvo se dolaznim bitovima iz ADC-a puni mikser1 i kad se on napuni određenom količinom bita, čiji se broj može regulisati podešivačem N brojača bita, sinhronizator isključuje punjenje miksera1 i automatski uključuje punjenje miksera2. Kada mikser1 završi obradu vrši se XOR-ovanje a istinski slučajan niz bita šalje u izlazni bafer. Pošto je mikser2 završio sa punjenjem uključuje se punjenje miksera1, a iz miksera2 se preraspodeljeni bitovima XOR-uju i šalju na izlaz. Postupak se na isti način nastavlja. Na taj način se ukupan broj bita iz ADC-a, posle izvršenog post-procesirsanja redukuje na pola i šalje na izlaz konstantnom brzinom.

Mada slučajnosti ne mogu nikada biti dokazive, posle najmanje 1 Mbita podataka, koji su bili sakupljeni pri svakom uzimanju uzoraka, uzorci su prošli sve NIST i FIPS statisticke testove slučajnosti a najbolji rezultati dobijeni su korišćenjem signala miksovane buke. U tabeli 1 prikazani su primeri rezultata testiranih slučajnih signala buke životne sredine, uzetih sa više različitih lokacija, dobijenih primenom metode MiBiS&XOR, a na Slika 4 dat je njihov grafički prikaz.

Sample	Statistical tests					
	Serial	Frequency	Runs	Entropy	Poker	Universal
#5	0.525	0.681	0.482	0.999	0.892	0.992
#4	0.311	0.651	0.390	0.993	0.797	0.989
#3	0.268	0.593	0.215	0.989	0.647	0.976
#1	0.478	0.323	0.686	0.976	0.249	0.961
#2	0.171	0.537	0.177	0.965	0.535	0.959

Tabela 1. Rezultati testiranja signala buke životne sredine nakon primene metode MiBiS&XOR

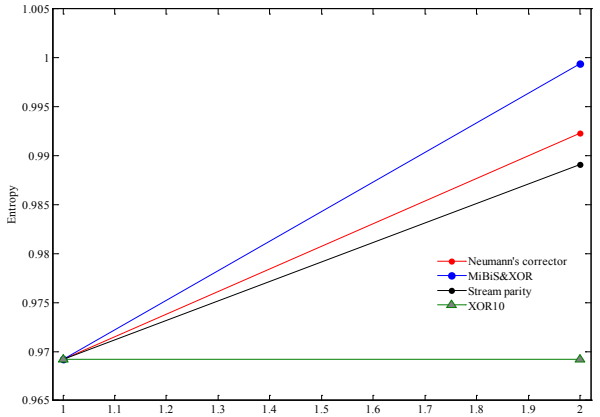
Ovim miksovanjem odnosno uticajem na dolazne bite dobija se takav razmeštaj bita koji omogućuje da se susedni bitovi, koji su u određenoj korelaciji, odvoje jedan od drugog, da se između njih ubace udaljeni bitovi sa kojima oni nisu u korelaciji i da se samim tim stvore idealni uslovi za XOR-ovanje dobijenih susednih bitova čime se značajno popravljaju karakteristike slučajnosti odnosno entropija izlaznog niza.



Slika 4. Grafički prikaz rezultata testiranja slučajnih analognih signala miksovane buke #5, buke na žurci #4, buke u podzemnom prolazu #3, buke velikog broja ljudi u pešačkoj zoni #1 i saobraćajne buke #2, nakon primene post-procesiranja

Upoređivanje metode MiBiS&XOR sa najčešće korišćenim metodama post-procesirsanja (Nojmanov korektor, paritet niza i XOR-ovanje LSB-a i MSB-a svakog desetog odmerka), potvrdilo je odličan kvalitet predstavljene metode. Posmatrani su rezultati primene različitih metoda na miksovani signal buke životne sredine (#5).

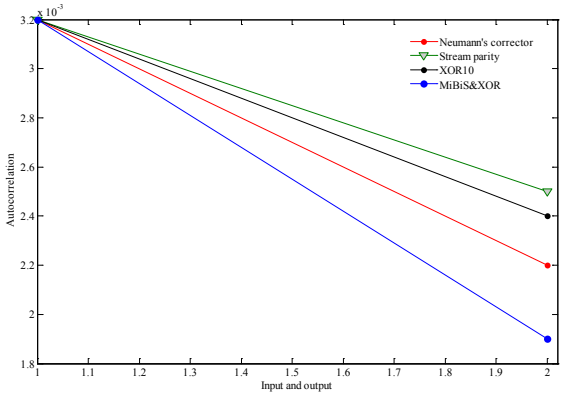
Entropija je najvažnija karakteristika svakog generatora slučajnih brojeva tako da njena vrednost određuje kvalitet TRNG-a. Rezultati testiranja pokazali su da je entropija koja se dobija prikazanom metodom MiBiS&XOR veća od entropija dobijenih upoređivanim metodama (Sl. 5).



Slika 5. Vrednosti entropija dobijenih primenom različitih metoda postprocesiranja

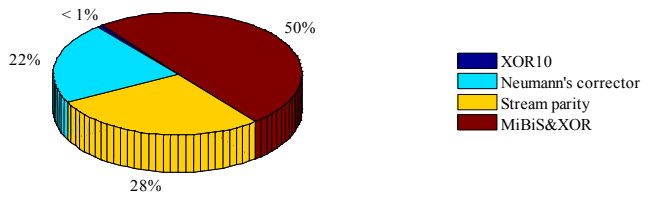
Eksperimentalna merenja su pokazala da se najmanja autokorelacija izlazlaznog niza dobija primenom tehnike MiBiS&XOR (Slika 6). Ako se u obzir uzme i sistemska greška, koji je kod niza dobijenog ovom metodom takođe najmanji, onda je potpuno logično zašto je ovom metodom dobijena najbolja entropija (Slika 5).

DOI: 10.15308/Synthesis-2015-97-100



Slika 6. Grafički prikaz srednjih apsolutnih vrednosti autokorelacije šuma miksovane buke pre i posle postprocesiranja različitim metodama

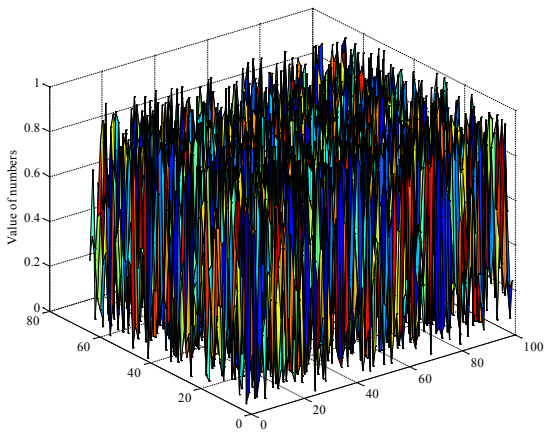
Procenat iskorišćenja bita, odnosno broj bita na izlazu iz TRNG-a u odnosu na broj bita na izlazu iz ADC-a, je kod metode MiBiS&XOR 50% i daleko je veći od od upoređivanih metoda (Sl. 7).



Slika 7. Uporedna analiza iskorišćenja bita iz ADCa

Brzina generisanja bita metodom MiBiS&XOR (352.8 Kb/s) je takođe najveća i u poređenju sa ostalim metodama *Neumann's corrector* (155 Kb/s), *stream parity* (200 Kb/s) i XOR10 (4.41 Kb/s) (za Nojmanov korektor i *stream parity* date su približne vrednosti) predstavlja značajno uvećanje.

Uporedna analiza rezultata pokazala je da metoda MiBiS&XOR daje odlične rezultate. Čak i kada su testovi imali tendenciju sabotaže, forsiranjem prostoperiodičnim fiksnim frekvencijama u mikrofonu, nisu povećane korelacije ili odstupanja. Na Sl. 8 prikazan je primer izgleda dobijenih rezultata istinski slučajnih brojeva sa vrednostima u rasponu od 0 do 1.



Slika 8. Uniformna raspodela dobijenih vrednosti slučajnih brojeva metodom MiBiS&XOR

Jedini nedostatak ove metode je taj što se konstantno generisanje bita ostvaruje tek pošto mikser1 završi prvi ciklus mešanja bita i pošto se izmešani bitovi XOR-uju, tako da se uključivanjem generatora ne dobija automatski izlazni niz istinski slučajnih bitova. U svakom slučaju svi elementi sekvenci generišu se nezavisno jedna od druge (statistička nezavisnost), a vrednosti sledećih sekvenci se ne mogu predvideti, bez obzira koliko je elemenata prethodno generisano.

3. REZIME

U ovom radu je, u cilju dobijanja istinski slučajnih bitova, prikazan pristup TRNG-ova koji je baziran na korišćenju standardnog hardvera personalnih desktop računara ili novijih generacija lap topova, tableta ili mobilnih smart telefona i primeni nove metode-post procesiranja.

Generatori istinski slučajnih brojeva korišćenjem prikazane metode obezbeđuju visok kvalitet slučajnih bita, veliku brzinu generisanja, nepredvidljivi su, nemaju periodičnu zavisnost i finansijski su pristupačni tako da su, iako namenjeni u kriptografske svrhe, pogodni za široku primenu u raznim oblastima od simulacija do igara na sreću.

LITERATURA

Gentle, J. (2004). *Random Number Generation and Monte Carlo Methods*. Berlin: Springer-Verlag Berlin Heidelberg.

Konar, S., & Biswas, A. (2005). Erratum to "Chirped Optical Pulse Propagation in saturating nonlinear media". *Optical and Quantum Electronics*, *37*(4), 905-918. DOI: 10.1007/s11082-004-8308-2

Mankad, H.S., & Pradhan, N.S. (2012). *Advances in Computer Science, Engineering & Applications*. DOI 10.1007/978-3-642-30157-5.

Morrison, R. (2001). Design of a true random number generator using audio input. *Journal of Cryptology*, *1*(1), 1-4.

Schindler, W, & Killmann, W. (2002). Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications. In Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems. August 2002 (431-449). London, UK: Springer-Verlag.

Walker J. (2006). HotBits: *Genuine random numbers, generated by radioactive decay*. Preuzeto 20.01.2015. sa https://www.fourmilab.ch/hotbits/

DOI: 10.15308/Synthesis-2015-97-100