Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI:
10.15308/SINTEZA-2014-995-1000

NOVA METODA DESTILACIJE GENERATORA ISTINSKI SLUČAJNIH IMPULSA NA BAZI ZVUČNE KARTICE RAČUNARA

Slaviša Nikolić
Elektrotehnička škola „Zemun", Srbija

Abstract:
Kvalitet generatora istinski slučajnih brojeva (TRNG) na bazi zvučne kartica računara pre svega zavisi od dve komponente: visine entropije „nepredvidljivog izvora" i funkcije post-procesnog postupka koja, kada se primeni na digitalizovani oblik slučajnog signala izvora, proizvodi rezultat koji je statistički vrlo blizu uniformnoj raspodeli. U ovom radu je prikazan metod dobijanja istinski slučajnih impulsa korišćenjem hardvera zvučne kartice računara, na čiji se audio ulaz preko njihovih ugrađenih mikrofona dovodi slučajni signal buke životne sredine a za post-procesiranje se koristi nov postupak raspoređivanja bita tzv. „miksovanje bita u koracima". Predstavljenim postupkom destilacije se na jednostavan i efikasan način dobija takav raspored bita kod koga su susedni ulazni biti, koji su u određenoj korelaciji, odvojeni i udaljeni jedni od drugih, čime se smanjuje ukupna autokorelacija a povećava entropija izlaznog bitskog niza.

Key words:
generator istinski slučajnih impulsa,
entropija,
zvučna kartica,
autokorelacija,
statistički testovi.

UVOD

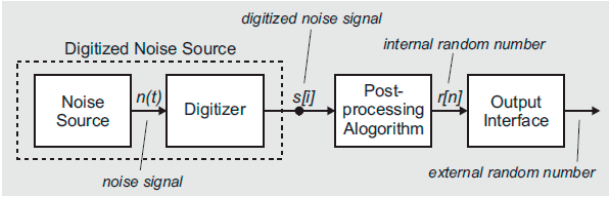
Slučajni brojevi su ključni sastojci čitavog niza oblasti, uključujući kriptografiju, simulacije, igre na sreću, uzorkovanje, donošenje odluka, medicinu i estetiku kao i umetnost. Najčešće korišćeni generatori slučajnih brojeva su generatori pseudo-slučajnih brojeva (PRNG). Generatori pseudo-slučajnih 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 (eng. *seed* – seme) [1]. 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. TRNGi se sa druge strane zasnivaju na nedeterminističkim izvorima kao što su radio šumovi [2], radioaktivno raspadanje [3], termalni šumovi generisani od strane poluprovodnika [4], termalni šumovi kod otpornika, fotoelektrični efekti ili razni kvantni fenomeni [5]. Takve prirodne pojave (analogni slučajni signali) se pojačavaju a onda nakon analogno-digitalne konverzije digitalno očitavaju i dalje koriste. Dobar kvalitet TRNGa zahteva i post-procesnu obradu mada ova komponenta nije neophodna u svim dizajnima (npr. TRNGs bazirani na kvantnim fenomenima). TRNGi imaju mnoge prednosti u odnosu na PRNG generatore. Prvo, nepredvidivost TRNG-a nudi bolje slučajne vrednosti. Drugo, TRNG nemaju periodičnu zavisnost, što je najvažnija osobina koju treba ispuniti kod strogih uslova za komunikaciju i šifrovanje.

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 analogni signal buke životne sredine. Prikazano je i korišćenje nove metode post-procesiranja tzv. „miksovanje bita u koracima", kojom se na inovativan način vrši promena rasporeda bita ulaznog niza a koja kao rezultat daje novi niz bita kod koga je razmeštaj bita takav da su susedni ulazni biti udaljeni jedni od drugih, čime se smanjuje korelacija a povećava ukupna entropija izlaznog bitskog niza. Statistička testiranja slucajnosti, pre svega ona koja se odnose na entropiju i autokorelaciju, vršena na nizovima bita dobijenim kao rezultat predlozene metode, potvrđuju odličan kvalitet izlaza TRNGa. Eksperimentalna testiranja su takođe pokazala da TRNGi na bazi zvučne kartice racunara, korišćenjem metode „miksovanja bita u koracima", imaju sposobnost da se suprostave procesima temperaturnih varijacija i mogu pozitivno da reaguju na neželjenu, ponekad zlonamerno izazvanu, determinističku buku.

PRINCIP RADA TRNGA

Rad TRNG-a se može podeliti u tri faze (Sl. 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 [6].



Sl. 1. Princip rada TRNGa

Prva faza rada TRNGa

U prvoj fazi rada TRNG-a neophodno je slučajne analogne veličine (signale) prevesti u digitalan oblik. Proces ili postupak koji omogućuje dobijanje zapisa neke analogne veličine u digitalnom obliku naziva se analogno-digitalna (A/D) konverzija. Tipično, proces A/D konverzije obuhvata odmeravanja analogne veličine u vremenu i po amplitudi.

Odmeravanje analognog signala *n(t)* vrši se u ritmu taktnog signala i na izlazu se dobija diskretni signal - to je diskretizacija analognog signala po vremenu. Analogni kontinualni signal se predstavlja nizom diskretnih odmeraka koji se uzimaju u tačno određenim trenucima vremena. Frekvencija odmeravanja treba da zadovolji *Nyquist*-ovu teoremu da ne bi došlo do preklapanja u spektru.

Kvantizacija je zaokruživanje amplitude odmeraka na najbližu dozvoljenu vrednost iz ukupnog opsega vrednosti, odnosno to je postupak određivanja amplitude pojedinih uzoraka. Kvantizacija smanjuje broj dozvoljenih (unapred definisanih) amplitudskih vrednosti. Broj nivoa kvantizacije je ograničen i određen ukupnim brojem bita po odmerku.

U koderu se vrši kodovanje, prema definisanom kodu i generisanje digitalnog signala *s[i]*, koji je pogodan za obradu i prenos u digitalnim sistemima. To je postupak dodeljivanja binarnog koda svakom kvantizacijskom nivou, odnosno to je dodeljivanje svakom odmerku određene kombinacije 0 i 1. Manji broj kvantizacijskih nivoa određen je manjim brojem bita potrebnih da se svaki odmerak predstavi i obrnuto.

Druga faza rada TRNGa (Tehnika postprocesiranja – destilacija entropije izvora)

U drugoj fazi se post-procesom izdvajanja (destilacija) eliminišu slabosti generisanja impulsa (npr. pojava dugih nizova nula ili jedinica) odnosno generisu se *interni (unutrasnji) slucajni brojevi r[n]*. Destilacija je proces stvaranja pouzdano nepredvidivih sekvenci iz nepouzdano nepredvidivih izvora sekvenci odnosno predstavlja poboljšanje entropije izvora po bitu. Sam proces je neophodan zbog nemogućnosti korišćenja kontinualnih signala izvora i dobijenih sekvenci u realnom vremenu. Sam proces je neophodan zbog nemogućnosti korišćenja kontinualnih signala izvora i dobijenih sekvenci u realnom vremenu. Post-procesiranjem se ustvari vrši transformisanje digitalizovanih slučajnih signala u ravnomerno raspoređene slučajne brojeve, čak i ako inicijalni signal ima značajne statističke nedostatke. Štaviše, post-procesiranjem se prikuplja sva entropija slučajnog izvora šuma i uvećava se za deo koji se dobija onemogućavanjem pojave dugih nizova nula i jedinica, koja se inače javlja kod digitalizovanih signala. Na ovaj način ispravljaju se loše osobine TRNG-a kao što su mala entropija (značajno manja od 1), velika pristrasnot – bias (značajno različit broj jedinica od broja nula) ili velika autokorelacija (značajno veća od 0).

Najpopularnije destilacione tehnike, pre svega zbog svoje jednostavnosti, su Von Neumann-ov korektor, Paritet niza i XOR korektor. Rezultati primene ovih metoda za različite kombinacije ulaznih parova bita, prikazani su u tabeli 1.

Tabela 1 Primena različitih tehnika post-procesiranja

Ulazni biti	Izlazni bit		
	Neumann	Parity	XOR
00	ništa	0	0
01	0	ništa	1
10	1	ništa	1
11	ništa	1	0

EKSPERIMENT I ANALIZA REZULTATA

Princip miksovanja bita

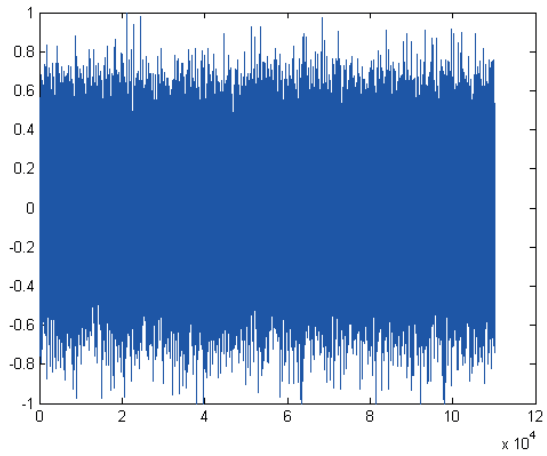
U ovom radu je, u cilju dobijanja istinski slučajnih bita, prikazan inovativan pristup TRNGima koji je baziran na korišćenju standardnog hardvera personalnih desktop računara ili novijih generacija lap topova, tableta ili mobilnih smart telefona i primeni nove metode-post procesiranja nazvanoj „miksovanje bita u koracima". Zadatak miksera je da prihvati izlaznu sekvencu bita iz ADCa, promeni raspored dolazećih bita, smanji autokorelaciju između bita i kao rezultat da izlazni niz bita sa većom entropijom u odnosu na entropiju ulaznog niza.

Kod ove metoda se kao fizički izvor slučajnosti 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)

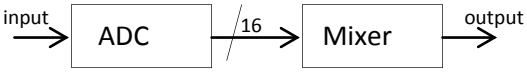
Za dobijanje istinski slučajnih bita koristila se zvučna kartica računara, na koju se preko mikrofona dovodi slučajni analogni signal buke. Kretanje, odnosno pomeranje raznih stvari, saobraćajna buka, razgovori većeg broja

ljudi kao i sva ova buka zajedno, koja predstavlja buku životne sredine (*Environmental Noise*), stvara veliki broj zvučnih talasa različitih frekfencija, amplituda i faza, koji prolazeći kroz vazduh i odbijajuće se od objekata stvaraju u mikrofonu nepredvidive amplitude. Analogni zvuk se u mikrofonu konvertuje u napon a onda nakon ADC-a u podatke u obliku bita. Na Sl. 2 prikazan je primer signala buke životne sredine na izlazu mikrofona odnosno ulazu ADCa.



Sl. 2. Snimljeni šum

Velikom brzinom odmereni, podaci odmeraka imaju nedozvoljeno visoka korelaciona svojstva. Ovo je očekivano jer se odmerava kontinualan i ponekad sporo promenljiv analogni signal. Međutim, postoje metode popravljanja entropije izlaznih bitskih vrednosti. U ovom radu korišćen je metod miksovanja kojim se vrši mešanje bitskog niza iz ADCa (Sl. 3) a kao rezultat dobija se novi niz bitova kod koga je razmeštaj bitova takav da su susedni biti udaljeni i geometrijski i vremenski jedni od drugih, čime se smanjuje korelacija a povećava 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,x**3**,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,x**4**,x3,x**5**,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,x**6**,x4,x**8**,x3,x**9**,x5,x**7**,x2 (tabela 2).



Sl. 3. Princip postprocesiranja korišćenjem miksera

Primenom istog postupka po završetku petog koraka dobija se sledeći raspored bita u ovim korakom nastalom nizu:x1,x**10**,x6,x**12**,x4,x**14**,x8,x**16**,x3,x**17**,x9,x**15**,x5,x**13**,x7,x**11**,x2. Sledeći koraci se ponavljaju na isti način sve dok se ne rasporede svi ulazni biti.

tabela 2 Postupak raspoređivanja bita u prva četiri koraka

Broj koraka miksovanja	Raspored bita
1st step	x1, x2
2nd step	x1, x3, x2
3rd step	x1, x4, x3, x5, x2
4th step	x1, x6, x4, x8, x3, x9, x5,x7,x2

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 $n = 1,2,3,\ldots,\infty$.

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

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

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

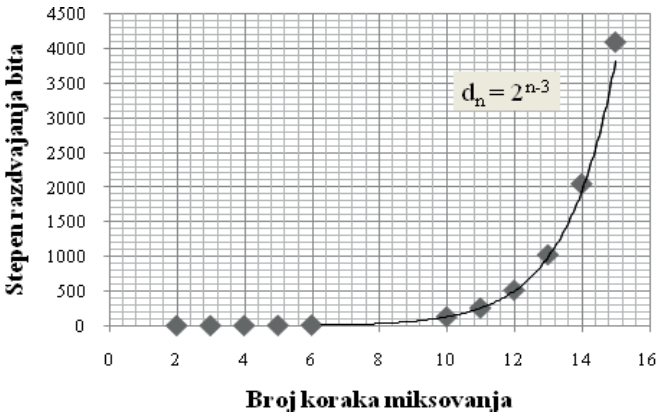
$$m_n = 2^{n-2} \quad (3)$$

Rastojanje ili razmak između uzastopnim rasporedom primljenih bita iz ADCa, se u principu povećava sa 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 biti čije je najmanje rastojanje u rasporedu redosleda primljenih bita dva (x6,x4 i x5,x7) što praktično znači da postoje susedni biti 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. 4.

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

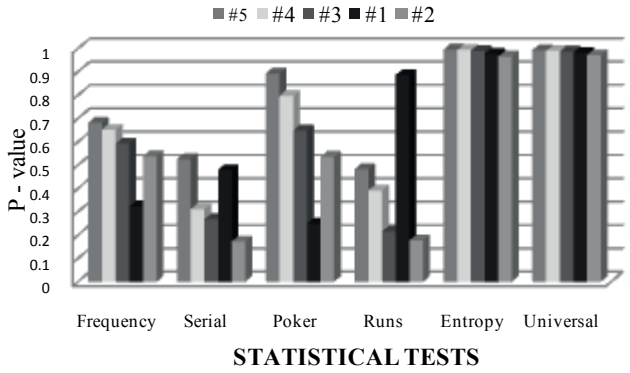
$$d_n = 2^{n-3} \quad (4)$$

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



Sl. 4. Grafički prikaz povećanja stepena razdvajanja bita po koracima

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. U tabeli 3 prikazani su primeri rezultata testiranih slučajnih signala buke životne sredine, uzetih sa više različitih lokacija, dobijenih primenom metode miksovanja a na Sl. 5 dat je njihov grafički prikaz.

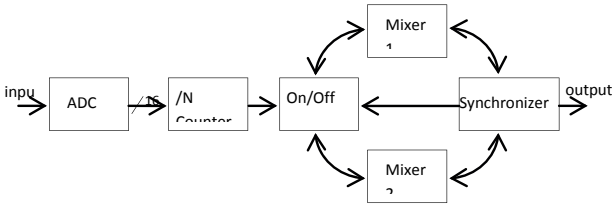


Sl. 5. Grafički prikaz rezultata testiranja slučajnih analognih signala miksovane buke #5, buke na žurci #4, buke u podzemnom prolazu #3, buke velikog broja ljudi u pešačkoj zoni #1 i saobraćajne buke #2, nakon primene post-procesiranja

Tabela 3 Rezultati testiranja signala buke životne sredine nakon primene metode miksovanja bita

Uzorci	Statistički testovi					
	Frequency	Serial	Poker	Runs	Entropy	Universal
#5	0.681	0.525	0.892	0.482	0.995	0.992
#4	0.651	0.311	0.796	0.390	0.993	0.989
#3	0.593	0.268	0.647	0.215	0.988	0.986
#1	0.323	0.478	0.248	0.886	0.976	0.981
#2	0.537	0.171	0.535	0.177	0.965	0.970

Preraspodelu bita predstavljenom metodom moguće je izvesti na prikazani način korišćenjem samo jednog miksera, međutim, takvim načinom miksovanja se gubi određeni broj bita zato što mikser nakon određene količine skupljenih ulaznih bita mora prestati sa primanjem bita jer mu je potrebno određeno vreme za mešanje. U ovom slučaju bi dolazni biti iz ADCa, sve dok traje obrada prihvaćenih bita, bili nepovratno izgubljeni. Rešenje je pronađeno korišćenjem dva nezavisna miksera koji naizmenično rade – Sl. 6.

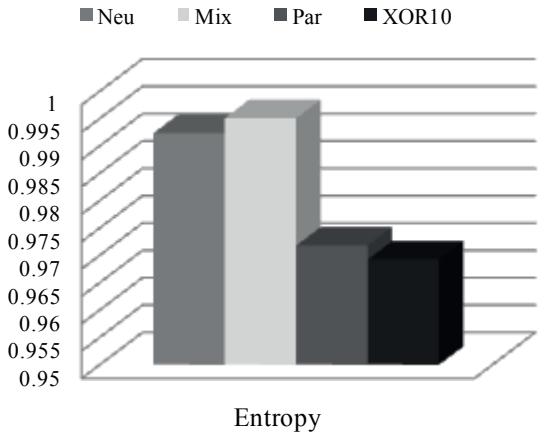


Sl. 6. Proces dobijanja slučajnih bita korišćenjem dva miksera

Uporedni rezultati

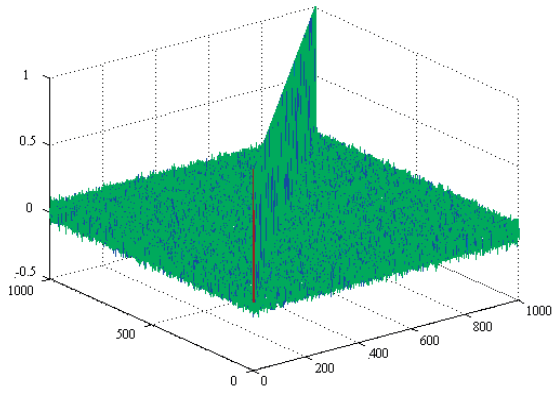
Upoređivanje metode miksovanja bita u koracima sa najčešće korišćenim metodama post-procesirsanja (Nojmanov korektor, paritet niza i XOR-ovanje LSB-a i MSB-a svakog desetog odmerka) potvrdilo je odličan kvalitet predstavljene metode. Posmatrani su rezultati primene različitih metoda na miksovani signal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

Entropija je najvažnija karakteristika svakog generatora slučajnih brojeva, bita ili impulsa odnosno nizova slučajnih brojeva i bita, tako da njena vrednost ustvari određuje kvalitet TRNGa. Rezultati testiranja pokazali su da je entropija koja se dobija novom prikazanom metodom *miksovanja* veća od entropija dobijenih upoređivanim metodama (Sl. 7).



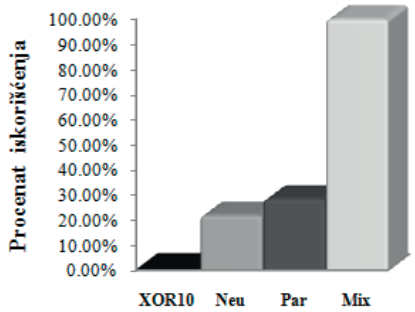
Sl. 7. Vrednosti entropija dobijenih primenom različitih metoda

Presudan uticaj na kvalitet izlaznog niza, samim tim podrazumevano i na entropiju, svakako imaju autokorelacija i bias. Eksperimentalna merenja su pokazala da se najmanja autokorelacija izlazlaznog niza dobija primenom tehnike miksovanja bita (Sl. 8). Ako se u obzir uzme i bias, koji je kod niza dobijenog ovom metodom takođe najmanji, onda je potpuno logično zašto je ovom metodom dobijena najbolja entropija (Sl. 7).



Sl. 8. Autokorelacija niza istinski slučajnih bita dobijenog metodom miksovanja bita

Procenat iskorišćenja bita na izlazu iz ADCa je kod metode miksovanja bita 100% i daleko je veći od upoređivanih metoda (Sl. 9).



Sl. 9. Uporedna analiza iskorišćenja bita iz ADCa

Brzina generisanja bita metodom Miksovanja je takođe najveća i u poređenju sa ostalim metodama (za Nojmanov korektor i Paritet niza date su približne vrednosti) prikazana je u tabeli 4.

Tabela 4 Brzina generisanja bita

Metod post-procesiranja	Brzina generisanja bita Kb/s
Miksovanje bita u koracima	705.60
Nojmanov korektor	155.00
Paritet niza	200.00
XOR10	4.41

Uporedna analiza rezultata pokazala je da metoda miksovanja bita u koracima daje odlične rezultate. Čak i kada su testovi imali tendenciju sabotaže, forsiranjem prostoperiodičnim fiksnim frekvencijama u mikrofonu, nisu povećane korelacije ili bias-i kada je N bilo veće od 5. Na ovaj način se proizvodi bitska brzina od 705.6 Kbit/s pri frekvenciji odmeravanja 44.1 KHz, što može biti dovoljno za mnoge kriptografske aplikacije. Na Sl. 10 prikazan je primer izgleda histograma dobijenih rezultata.

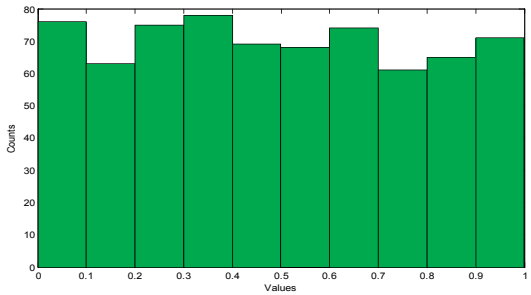


Fig. 14. Histogram uniformne raspodele dobijenih vrednosti slučajnih brojeva

Jedini nedostatak ove metode je taj što se konstantno generisanje bita ostvaruje tek pošto mikser1 završi prvi ciklus mešanja bita tako da se uključivanjem generatora ne dobija automatski izlazni niz istinski slučajnih bita. Ovo vreme kašnjenja je vrlo kratko i zavisi pre svega od dužine bloka sekvenci i brzine rada procesora računara. 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.

ZAKLJUČAK

U ovom radu je, u cilju dobijanja istinski slučajnih bita, prikazan inovativan pristup TRNGima 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 impulsa korišćenjem prikazane metode obezbeđuju visok kvalitet slučajnih bita, veliku brzinu generisanja, nepredvidljivi su i nemaju periodičnu zavisnost, tako da su pogodni za široku primenu u raznim oblastima od kriptografije preko simulacija do igara na sreću. Zbog činjenice da su dostupni širokim narodnim masama i obrazovnim ustanovama mogu se odlično iskoristiti za nova istraživanja, eksperimentisanje i edukaciju.

LITERATURA

[1] Gentle J (2004) Random Number Generation and Monte Carlo Methods (Statistics and Computing). Springer-Verlag, Berlin, Germany

[2] HAAHR, Mads: *Random.org* [online]. 2012, [cited 2012 -10-13]. Available at www.random.org.

[3] Lavarnd. http://www.fourmilab.ch/hotbits/.

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

[5] Menezer A.J., Van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptograp¬hy. CRC-Press, 1997.- 780 c.

[6] Schindler W, Killmann W (2001) AIS 31: Functionality classes and evaluation methodology for true (physical) random number generators, version 3.1, Bundesamt fur Sicherheit in der Informationstechnik (BSI), Bon

A NEW METHOD OF DISTILLATION OF TRUE RANDOM PULSE GENERATORS BASED ON SOUND CARD

Abstract:
Quality of true random number generators (TRNGs) based on a sound card primarily depends of two components: an „unpredictable" source with high entropy, and a post processing function which, when used on a digitalized form of a random signal source, produces a result that is statistically very close to the uniform distribution. This paper presents a new method of obtaining a true random pulses using hardware of a computer sound card, on which the audio input through the use of built-in microphone brings a random environmental noise signal and for post-processing a new procedure of distributing bits is used or so called "mixing bits in steps". With the presented distillation procedure, on a simple and efficient way, such a distribution of bits is obtained in which the adjacent input bits, which are in a certain correlation, separated and divided one from another, by which the total autocorrelation is reduced and entropy of output bit sequence is increased.

Key words:
True Random Number Generator,
Entropy,
Sound Card,
Autocorrelation,
Statistical Tests.