GENERATORI SLUČAJNIH SEKVENCI I NJIHOV UTICAJ NA SIGURNOST
GENERATORS OF RANDOM SEQUENCES AND THEIR IMPACT ON SECURITY

Saša Adamović, Miloš Milenković, Marko Šarac, Dalibor Radovanović- *University Singidunum, Danijelova 32, Beograd, Serbia*

Sadržaj – *U ovom radu se analiziraju generatori slučajnih sekvenci (eng. true random number generator, **TRNG**). U poređenju sa PRNG (eng. pseudorandom number generator, **PRNG**), TRNG je ekstrakt slulajnosti završnog procesa fizičkih pojava uvedenih u računar. Entropija izvora obično se sastoji od neke fizičke količine informacije, kao što su atmosferski šum, proteklo vreme radioaktivnog raspadanja (npr. Hotbits), termički šum poluprovodničkih dioda ili frekvencija nestabilnosti oscilatora. Zbog velike nepredvidivosti ovakvih izvora, u radu se razmatra korišćenje procesa destilacije da bi se prevladale slabosti, u slučaju upotrebe ovako generisanih nizova za kriptografske potrebe (npr. pojava dugih nizova nula ili jedinica).*

Abstract - *In this paper analyzes the random sequence generator (eng. true random number generator, TRNG). In comparison with the PRNG (English pseudorandom number generator, PRNG), TRNG randomness extract the final process of physical phenomena introduced in the computer. Entropy sources usually consist of some physical quantities of information, such as atmospheric noise, the elapsed time of radioactive decay (eng Hotbits), thermal noise of semiconductor diode or oscillator frequency instability. Because of the unpredictability of these large sources, the paper discusses the use of the distillation process to overcome weaknesses in the case of the use of such generated sequences for cryptographic purposes (eg appearance of a long series of zero or unit).*

1. UVOD

U savremenim sistemima komunikacije, postoji konstantna potreba za povećanjem propusnosti i količine prenesenih podataka. Sa ciljem da se obezbedi sigurna komunikacija u takvim sistemima, podaci moraju biti šifrovani. Kriptografski algoritmi moraju zadovoljiti zahteve efikasnosti. Npr. u internet protokolu (IP) koriste se blokovski algoritmi za šifrovanje, slučajni inicijalni vector je neophodan za svaki šifrovani paket. Dužina slučajne sekvence zavisi od veličine bloka koji koristi algoritam za šifrovanje. Za blokovske šifarske algoritme, kao što je AES dužina je 128 bita. Današnja brzina komunikacionih sistema može biti nekoliko desetina Gbit/s, a maksimalna veličina paketa 1500 bajta [1], generator slučajnih brojeva (TRNG) moraju imati minimalnu brzinu od 100Mbit/s da bi postigli rad šifarskog sistema na komunikacionoj brzini od 10Gbit/s.

Potreba za slučajnim i pseudo-slučajnim brojevima javila se zbog velike primene u kriptografskim sistemima. Zajedničko za sve kriptografske sisteme je generisanje ključeva na slučajan način. Mnogi kriptografski protokoli, protokoli za autentifikaciju, protokoli za generisanje digitalnog potpisa koriste na ulazu slučajne ili pseudo slučajne vrednosti. U radu se razmatra o nasumičnosti generatora potpuno slučajnih vrednosti, koji se mogu koristiti za mnoge svrhe, uključujući kriptografiju, modelovanje i simulacije u aplikacijama.

2. NASUMIČNOST

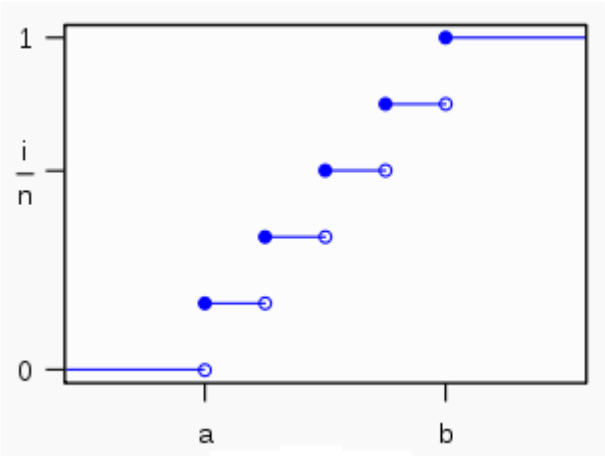
Slučajna bitna sekvenca može se tumačiti kao rezultat bacanja novčića koji je označen sa "1" ili "0", gde svaki ishod (0 ili 1) ima verovatnoću tačno ½. Bacanje novčića predstavlja savršen generator slučajnih vrednosti jer "1" i "0" će biti nasumično raspodeljene (ujednačena raspodela). Svi elementi sekvenci generišu se nezavisno jedna od druge (statistička nezavisnost), a vrednosti sledećih sekvenci se ne mogu predvideti, bez obzira koliko je elemenata prethodno generisano.

2.1 Uniformna distribucija (ujednačena raspodela)

U teoriji verovatnoće i statistike, diskretna uniformna raspodela je diskretna verovatnoća raspodele koja se može okarakterisati rekavši da su sve vrednosti konačan skup mogućih vrednosti podjednako verovatnih.

Diskretnu ujednačenu raspodelu realnih u slučaju vrednosti slučajne promenljive moguće je izraziti preko kumulativne funkcije raspodele:

$$F(k;a,b,n)=\frac{1}{n}\sum_{i=1}^{n}H(k-k_i)$$



Slika 1. Kumulativna funkcija raspodele

$n=5, n=b-a+1;$

2.2 Statistička nezavisnost teorije verovatnoće

U teoriji verovatnoće, dva su događaja nezavisna intuitivno ukoliko pojava jednog događaja ne čini ni više ni manje verovatno da dođe do drugog.

Dva događaja A i B su nezavisni ako I samo ako je Pr(A ∩ B) = Pr(A)Pr(B). Opštije rečeno, bilo koji skup događaja, verovatno više od dva, su međusobno nezavisni ako i samo ako za bilo koji konačan podskup A1, …..,An imamo:

$$\Pr\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} \Pr\left(A_i\right)$$

Navedeno pravilo se zove množenje nezavisnih događaja.

3. NEPREDVIDIVOST

Slučajni i pseudo slučajni brojevi generisani za kriptografske sisteme moraju biti nepredvidivi. U slučaju pseudo generatora, ako je sid ili inicijalno stanje generatora nepoznato, sledeće binarne sekvence će biti nepredvidive i pored bilo kog znanja o prethodnim binarnim sekvencama.

Takođe, ne treba da bude moguće da se utvrde sidovi na osnovu prethodno generisanih sekvenci. Između sidova i binarnih sekvenci nema korelacije, svaki bit sekvence treba da bude potpuno nezavisan, čija je verovatnoća ½.

Entropija nepredvidivosti slučajne promenjive X sa verovatnćom $p_i, \ldots, p_n$ je definisana kao:

$$H\left(X\right) = -\sum_{i=1}^{n} p_i \log p_i$$

4. VRSTE GENERATORA

Postoje dva osnovna pristupa za generisanje slučajnih brojeva korišćenjem računara: pseudo slučajni generatori brojeva (PRNG) i istinito slučajni generatori brojeva (TRNG). Svaki od navedenih pristupa ima svoje prednosti i mane.

Karakteristike TRNG su poprilično drugačije od PRNG, TRNG su neefikasni u odnosu na PRNG. Potrebno im je znatno više vremena da proizvedu određen broj slučajnosti.

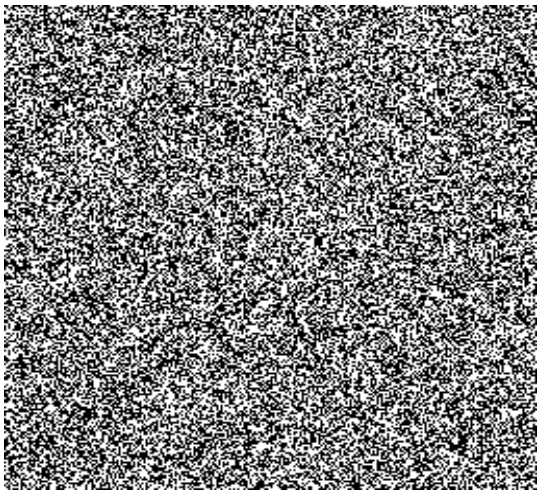
Slučajne promenljive dobijene TRNG su potpuno nedeterminističke, što znači da dati niz slučajnih promenljivih nije moguće reprodukovati [4]. Još jedna bitna karakteristika ovih generatora slučajnosti jeste izbegnuta perioda datih slučajnih nizova.

5. KOMPARATIVNA ANALIZA PRNG SA TRNG

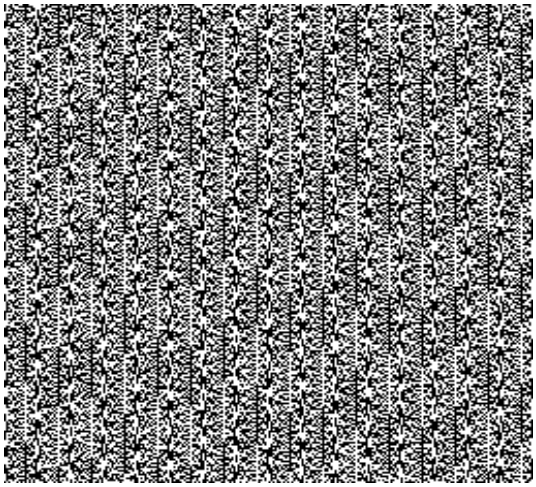
U tabeli 1 su prikazane karakteristike dva tipa proizvoljnog broja generator.

Karakteristike	PRNG	TRNG
Efikasnost	da	ne
Deteminizam	da	ne
Periodičnost	da	ne

Navedene karakteristike čine TRNG pogodnijem za veći skup aplikacija u odnosu na PRNG koji bi bio nepodoban za aplikacije kao što su razni sistemi za šifrovanje podataka i igre na sreću. Nasuprot tome, loša eefikasnost i nedeterministička priroda TRNG čini ih manje pogodnim za simulacije i modeliranje aplikacija, koje često zahtevaju više podataka nego što je moguće proizvesti sa TRNG.



Slika 2. Grafička analiza rezultata TRNG



Slika 3. Grafička analiza rezultata PRNG

6. GENERATORI SLUČAJNIH BROJEVA (TRNG)

RNG generatori koriste nedeterministički izvor slučajnosti (tj. entropiju izvora), korišćenjem procesa destilacije nad entropijom izvora preovlađuju se slabosti generisanja neslučajnih brojeva (npr. Pojava dugih nizova nula ili jedinica).

Entropija izvora obično se sastoji od neke fizičke veličine, kao što su šum, vreme izvršavanja korisničkih procesa (npr. taster miša ili tastature) ili kvantni efekti u poluprovodniku.

Pri generisanju slučajnih sekvenci razne kombinacije ovih ulaza se mogu koristiti. Rezultat TRNG generatora može se koristiti kao slučajan broj, ili može predstavljati sid pseudoslučajnih generatora (PRNG). Da bi se rezultat koristio direktno (bez dalje obrade), izlaz iz RNG mora da zadovolji stroge kriterijume nasumičnosti mereno statističkim

testovima kako bi se utvrdilo da se fizički izvori RNG ulaza pojavljuju nasumično.

Na primer, fizički izvor kao što je elektronski šum može da sadrži superpoziciju redovne strukture, kao što su talasi ili druge periodične pojave, koji mogu biti slučajni, ali primenom statističkih testova oni nisu posledica slučajnosti.

Za kriptografske svrhe, izlaz RNGa treba da bude nepredvidiv. Međutim, neki fizički izvori kao što je vremenski vektor mogu biti prilično predvidivi. Ovakvi problemi rešavaju se kombinovanjem različitih izvora i dobijen rezultat se daje na ulaz RNGa [2]. Međutim postoji mogućnost da dobijeni rezultati RNGa ne mogu proći neke od statističkih testova.

6. PROCES DESTILACIJE ENTROPIJE IZVORA

Kombinovanje različitih izvora (entropija izvora) i procesa destilacije, rezultira sa binarnim sekvencama velike verovatnoće nepredvidivosti, čak i ako je izvor bita sa malom verovatnoćom nepredvidivosti.

Destilacija je proces stvaranja pouzdano nepredvidivih sekvenci iz nepouzdano nepredvidivog izvora sekvenci ili predstavlja poboljšanje entropije izvora po bitu. Sam proces je neophodan zbog nemogućnosti kontinualne analize izvora i dobijenih sekvenci u realnom vremenu. Na ovaj način ispravljamo loše osobine TRNG.

Jedan od glavnih metoda u procesu destilacije je statističko uklanjanje grešaka koje se bazira na algoritmu mapiranja prelaza (*transition mapping*). Analiziraju se po dva bita zajedno i u slučaju da postoji prelaz između dva bita (*01 - 10*) samo jedan od njih prihvata se kao slučajni. Ako nema prelaza (*00 - 11*) bitovi se odbacuju kao neslučajni. Von Neumann je osmislio kompletan algoritam i on u potpunosti uklanja pojavu dugih nizova 0 ili 1.

Drugi način je paritet niza (*stream parity*) slika 4. koji se realizuje na sledeći način. Nizovi se dele na parove zatim se određuje paritet svakog para. Parovi kod kojih je paritet različit odbacuje se, a kod kojih je isti zadržava se samo prvi bit. Bitovi koji nisu odbačeni čine niz koji ulazi u sledeći korak. U zavisnosti od kvaliteta dobijene kompresije entropije izvora određuje se stopa eksponencijalnog skraćenja polaznog niza.

Upotrebom procesa destilacije, poboljšavamo entropiju izvora što može biti dobra polazna tačka za bolje slučajne ili pseudo slučajne sekvence. Ovakvom vrstom digitalne post obrade podataka [3] obezbeđujemo uniformnost prikazano na slici 1. i izlaz prevazilazi određene korelacije ili statističku zavisnost izazvanu od hardverskog izvora zaista slučajnih podataka.Na ovaj način obezbeđujemo i analiziramo bezbedne, efikasne i jedinstvene primere nasumičnosti.

7. ZAKLJUČAK

U današnjem svetu savremeni računari i razna bezbednosna rešenja [6] oslanjaju se na kriptografske mehanizme. Generisanje visokog kvaliteta slučajnosti je vitalni (a možda i najteži) korak mnogih kriptografskih operacija i zbog toga je naglašena potreba za pažljivim dizajnom generatora slučajnosti. U radu su navedeni svi osnovni bezbednosni aspekti distribuiranih slučajnih sekvenci.

Bezbednost kriptografskih sistema neće da se zasniva na čuvanju tajnosti algoritma već isključivo se čuva tajni ključ gde tajnost zavisi direktno od kvaliteta nepredvidljivosti tajnih podataka.

Proces generisanja zaista slučajnih podataka u deterministčkom okruženju računarskih sistema ili u jednom čipu je izuzetno teško i sporo, tj.moguće je samo malu količinu podataka generisati u razumnom roku..

Teorija nasumičnosti donosi zanimljive ideje i rešenja u oblasti destilacije (post-procesiranja podataka) zaista slučajnih podataka. Sva rešenja se značajno razlikuju i imaju svoje prednosti i mane koje treba pažljivo razmotriti pre njihove praktične primene.

LITERATURA

[1] J. D. Goli´c, “New methods for digital generation and postprocessing of random data,” IEEE Trans. Comput., vol. 55, no. 10, pp. 1271–1229, 2006.

[2] NIST, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” NIST, Special Publication 800-22, Oct. 2000.

[3] J. Bouda, J. Krhovj´ak, V. Maty´aˇs, and P. ˇSvenda. Towards True Random Number Generation in Mobile Environments. Submitted to the special issue of Computing. Springer, 2009.

[4] G. Marsaglia, “Diehard: A battery of tests of randomness,”1996, available at: http://stat.fsu.edu/pub/diehard/.

[5] W. Aiello, S. Rajagopalan, and R. Venkatesan. Design of Practical and Provably Good Random Number Generators. In 5th Annual ACM-SIAM Symposium of Discrete Algorithms, pages 1–8, 1995.

[6] H. Bock, M. Bucci, and R. Luzzi. An Offset-Compensated Oscillator- Based Random Bit Source for Security Applications. In Cryptographic Hardware and Embedded Systems (CHES) 2004, volume 3156 of Lecture Notes in Computer Science, pages 268–281. Springer, 2004.

[7] E. Hoffman. Random number generator. 5706218 USA, 06. 01 1998.

[8] M. Bucci and R. Luzzi, ”Design of Testable Random Bit Generators”, Cryptographic Hardware and Embedded Systems - CHES 2005, Lecture Notes in Computer Science, vol.3659, pp.147-156, Springer- Verlag, 2005.

[9] B. Sklar, Digital Communications - Fundamentals and Applications, Second Edition. Prentice Hall PTR, 2001.