AKTET **ISSN 2073-2244**
Journal of Institute Alb-Shkenca **www.alb-shkenca.org**
Revistë Shkencore e Institutit Alb-Shkenca

GJENERATORËT E NUMRAVE TË RASTIT ME SISTEME KAOTIKE DINAMIKE
RANDOM NUMBER GENERATORS WITH CHAOTIC DYNAMIC SYSTEMS

TONI STOJANOVSKI[1], AJET REXHEPI[2]
[1] Faculty of Informatics; European University, 68 Kliment Ohridski Bld, Skopje; MACEDONIA
[2] Public High School "Drita", 2 Rudnicka Str, Kërçovë, MACEDONIA
toni.stojanovski@eurm.edu.mk, , ajetrexhepi@yahoo.com

AKTET VI, 2: 109 - 113, 2013

PËRMBLEDHJE
Gjeneratorët e numrave të rastit përdoren në shumë fusha, siç janë: simulimet kompjuterike, teknikat Monte-Carlo në analizën numerike, gjenerimi i test-problemeve për vlerësimin e algoritmeve kompjuterike dhe më së shumti në sistemet kriptografike. Siguria kriptografike po bëhet gjithnjë më e rëndësishme në shumë aplikacione të internetit, siç janë: posta elektronike, tregtia elektronike, administrata elektronike etj. Për të siguruar që një gjenerator i numrave të rastit të jetë i sigurt kriptografisht, të dhënat në dalje duhet të jenë statistikisht të pavarura dhe të paparashikueshme. Qëllimi kryesor i këtij hulumtimi është analiza e zbatimit të një mape lineare, të ndarë në segmente (*piecewise linear map*) me tri rajone për gjenerimin e numrave të rastit. Për një bashkësi të pafundme të numërueshme të parametrave, kjo mapë bëhet një burim Markov, entropia e të cilit mund të llogaritet matematikisht. Ky dokument thellon studimet e bëra deri tani, duke e shmangur nevojën për analiza statistikore.
Fjalët çelës: Gjeneratorët e numrave të rastit, Sistemet kaotike-dinamike, Entropia.

SUMMARY
Random number generators are used in many fields such as computer simulations, Monte-Carlo techniques in numerical analysis, generation of test problems for evaluation of computer algorithms, and most notably in cryptography. Cryptographic security is becoming increasingly important in many new Internet applications such as e-mail, e-commerce, e-government etc. To ensure that a random number generator is cryptographically safe, output data must be statistically independent and unpredictable. The main objective of this research is analyses of applicability of a piecewise linear map with three regions for random number generation. We do not rely on statistical test to prove the randomness of the random number generator. Finally, we explain our approach for calculation of information entropy as a measure for the quality of chaotic generators of true random numbers, and thus avoid the need for statistical tests.
Key-words: Random Number Generators, Dynamic Chaotic Systems, Entropy.

HYRJE

Praktikisht është shumë vështirë dhënia e ndonjë përkufizimi rreth asaj se çka është numri i rastit, edhe pse duket shumë thjesht në shikim të parë. Numër i rastit mund të quhet numri që gjenerohet nga ndonjë proces, dalja e të cilit është e paparashikueshme dhe i cili nuk mund të riprodhohet përsëri. Megjithatë ekzistojnë disa kritere që duhet t'i plotësojë ndonjë sekuencë numrash në mënyrë që të konsiderohet si e rastit:

- Paparashikueshmëria;
- Pavarësia;
- Të qenit e pastrukturë.

Kriptografia është disiplinë shkencore e cila merret me studimin e metodave për dërgimin e të dhënave në një formë të kuptueshme vetëm për marrësit. Fjala është me origjinë greke dhe do

të thotë shkrim i fshehur. Detyra themelore e kriptografisë është që të mundësojë komunikimin ndërmjet dy personave mbi kanalin e komunikimit të pasigurt të mos mund ta kuptojë një palë e tretë. Mesazhi që dërgohet quhet një tekst i hapur (*PLAINTEXT*). Dërguesi transformon tekstin e hapur duke përdorur një çelës paraprakisht të njohur. Kjo metodë quhet enkriptim, ndërsa rezultati quhet kriptogram (*ciphertext*). Personi i tretë mund të mësojë përmbajtjen e kriptogramit, por jo edhe tekstin e hapur. Ndryshe nga ai, marrësi e di se çelësi me të cilin mesazhi është koduar mund të dekriptojë mesazhin dhe të përcaktojë tekstin e hapur.

Për dallim nga kriptografia, kriptoanaliza është një disiplinë shkencore që studion procedurat për leximin e mesazheve të koduara, pa e ditur çelësin. Algoritmi kriptografik është i përbërë nga dy funksione matematikore, një për të kriptuar dhe një për të dekriptuar.

Qëllimet kryesore të kriptografisë janë [1]:

• ruajtja e konfidencialitetit të të dhënave – në drejtim të të dhënave mund të kenë akses vetëm personat e autorizuar,

• ruajtja e integritetit të të dhënave - parandalohet ndryshimi i fshehur i të dhënave

• kontrollet e identitetit - kontrollon nëse pjesëmarrësit në komunikim janë në të vërtetë ata që pretendojnë të jenë

• pengimi i pjesëmarrësve në komunikim të heqin dorë nga postet e tyre të mëparshme.

Çështja e gjenerimit të numrave të rastit merr vend të rëndësishëm në implementimin e sistemeve kriptografike. Numrat e rastit nevojiten sidomos për protokollet për autentikim, gjenerimit të çelësave, në skemat e nënshkrimeve digjitale madje edhe në skemat e në disa algoritme për enkriptim. Në të gjitha këto aplikime, siguria është shumë e varur nga cilësia e burimit të numrave të rastit. Cilësia e numrave të gjeneruar vërtetohen nga testet statistikore. Përveç kësaj, nga gjeneratorët e përdorur në kriptografi gjithashtu kërkohet paparashikueshmëria.

Është e njohur mirë se shumica e sulmeve janë të drejtuara drejt implementimeve të algoritmeve kriptografike dhe jo drejt algoritmit vetë [2]. Kjo do të thotë se një vëmendje e veçantë duhet të trajtojë shmangien e dobësive që do të kishin ndihmuar sulmuesin të rrëzojë sistemin .

MATERIALET DHE METODAT

Gjeneratorët e numrave të rastit janë përdorur në shumë fusha të tilla si simulimet kompjuterike, teknikat Monte-Carlo në analizën numerike, gjenerimi i test-problemeve për vlerësimin e algoritmeve kompjuterike etj. TRNG (*True random Number Generator*) cilësor ndihmon në përmirësimin e rezultateve në këto aplikacione dhe është shumë i rëndësishme për sigurinë kriptografike. Për të siguruar që gjeneratori i numrave të rastit të jetë i sigurt, të dhënat *output* duhet të jenë statistikisht të pavaruraa dhe të paparashikueshme. Protokolli kriptografik varet nga paparashikueshmëria e çelësit sekret, i cili është produkt i një gjeneratori të numrave të rastit. Nëse një sulmues mund të parashikojë vlerën e një protokolli të rëndësishëm do ta ketë shumë më të lehtë për ta thyer. Prandaj është shumë e rëndësishme që gjenerimi i çelësave të jetë nga një burim vërtetë i rastit. Nga ana tjetër, testet statistikore përcaktojnë nëse sekuenca të veçanta posedojnë një karakteristikë të caktuar të cilën do ta posedonte një sekuencë e rastit ose jo. Midis testeve më të njohura janë FIPS-140-1 i NIST dhe testi Diehard.

Në këtë punim si bazë janë marrë një numër i konsiderueshëm punimesh që kanë për temë gjenerimin e numrave të rastit, aplikimin e tyre në kriptografi dhe rëndësinë e kaosit në këtë drejtim. Mes tjerash, aty bëjnë pjesë edhe disa punime që propozojnë shfrytëzimin e sistemeve kaotike-dinamike gjatë gjenerimit të numrave me qëllim rritjen e sigurisë të sistemit kriptografik, siç janë:

Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos nga S. Callegari, R. Rovatti dhe G. Setti [3], *Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems* nga F. Pareschi, G. Setti dhe R. Rovatti [4], *Invariant Measures of Tunable Chaotic Sources: Robustness Analysis and Efficient*

Estimation nga T. Addabbo, A. Fort, D. Papini, S. Rocchi dhe V. Vignoli [5].

Siç përmendëm edhe në fillim, qëllimi kryesor i punimit është të mundësojë që vlerësimi i gjeneratorëve të numrave të rastit të bëhet në një mënyre empirike. Ashtu ne do t'u shmangemi testeve statistikore të cilat nuk na japin informacionin e sigurt për kualitetin e gjeneratorëve. Është edhe e qartë pse. Ne mundemi ta testojmë gjeneratorin me një numër të madh të testeve të ndryshme, mirëpo asnjëherë nuk do të dimë çfarë rezultati do të na jepte testi qe nuk e kemi bërë. A nga ana tjetër, nuk jemi në gjendje për një gjenerator t'i bëjmë të gjitha testimet e mundshme. Në mënyrën që propozohet në këtë punim, cilësinë e gjeneratorit të numrave të rastit do ta vlerësojmë në bazë të llogaritjeve të sakta që do t'i bëjmë. Duhet të përmendim se pse do t'i përdorim kaosin, sistemet kaotike-dinamike dhe mapat *piecewise* lineare. Që nga fillimi i hulumtimit së kaosit deri më sot, paparashikueshmëria e kaosit është një temë qendrore. Besohet gjerësisht dhe pretendohet nga shumë filozofë, matematikanë dhe fizikanë se kaosi ka një implikim të ri për paparashikueshmërinë, që do të thotë se sistemet kaotike janë të paparashikueshme në një mënyrë që sistemet e tjera deterministike nuk janë. Kaosi është përmendur shpesh në teorinë e sistemeve dinamike. Sistemi dinamik është një model matematikor i cili përbëhet nga një X hapësirë (hapësirë fazë - një hapësirë ku të gjitha gjendjet e mundshme të sistemit janë të përfaqësuara). Sistemet dinamike shpesh janë modele të sistemeve natyrore. Ka lloje të ndryshme të paparashikueshmërisë në sistemet dinamike. Sipas një koncepti të paparashikueshmërisë, sistemi është i paparashikueshëm, kur një grup i kushteve fillestare përhapet mbi një diametër që përfaqëson saktësinë e parashikimit. Kur kjo ndodh,sistemi është i paparashikueshëm në kuptimin që parashikimi i bazuar në ndonjë paketë me kushtet fillestare është aq i pasaktë saqë është e pamundur për të përcaktuar rezultatin e sistemit me saktësinë e dëshiruar. Një koncept i paparashikueshmërisë, është koncepti i probabilitetit. Sipas këtij koncepti, jo vetëm që është e pamundur të parashikohet me siguri, në cilin rajon të sistemit gjendja do të jetë, por se njohja e kushteve fillestare as e rrit e as e zvogëlon probabiliteti që gjendja është në një rajon të caktuar. Hulumtimi i mapave jolineare diskrete, si që janë mapat *piecewise* lineare paraqesin një kontribut interesant në zhvillimin e teorisë së sistemeve dinamike, me shumë aplikacione të mundshme në shkencë dhe inxhinieri. Shumë sisteme fizike dhe inxhinierike janë treguar të jenë të përfaqësuar më së miri nga mapat *piecewise* ku gjendja diskrete hapësirë-kohë është e ndarë në dy ose më shumë pjesë të realizuara me forma të ndryshme funksionale. Gjetja e rajoneve kaotike në mapat diskrete është një fushë shumë interesante në teorinë e sistemeve dinamike.

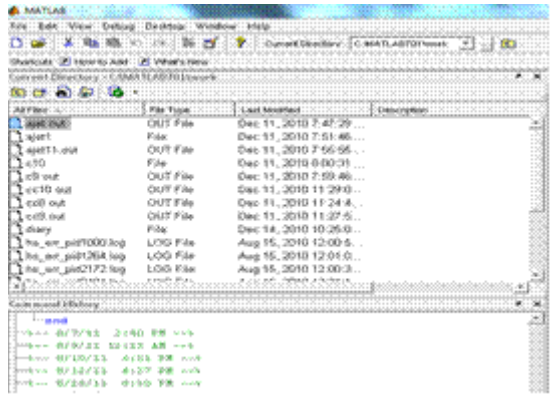

Fig. 1. Kodi në MATLAB

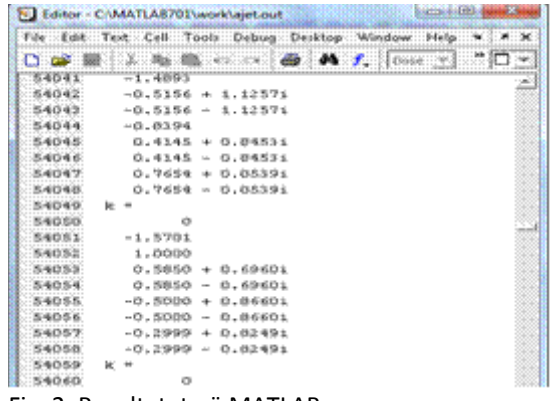

Fig. 2. Rezultatet në MATLAB

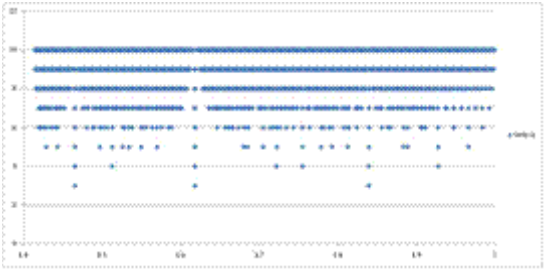

Fig.3. Rezultatet në MATLAB në formë grafike

REZULTATET DHE DISKUTIMI

Qëllimi kryesor i hulumtimit është analiza e zbatimit të mapave *piecewise* lineare me tri rajone për të gjeneruar numra të rastit. Në vijim janë nënqëllimet që kontribuojnë në arritjen e qëllimit kryesor. Do të përkufizohet një grup i caktuar i polinomeve rrënjët e të cilit janë vlerat e parametrave për të cilat mapat sillen si burime të Markovit të informacionit. Në MATLAB është punuar kodi për zgjidhjen e ekuacioneve polinomiale. Pastaj në MS Excel janë punuar llogaritjet dhe përfaqësimet grafike të shpërndarjes së probabilitetit të gjendjes (*pdf - probability distribution function*) të mapave kaotike. Llogaritja e *pdf* është vendimtare për arsyeshmërinë e hulumtimit. Më pas do të pasojnë llogaritjet e probabiliteteve të tranzicionit të burimeve Markov.

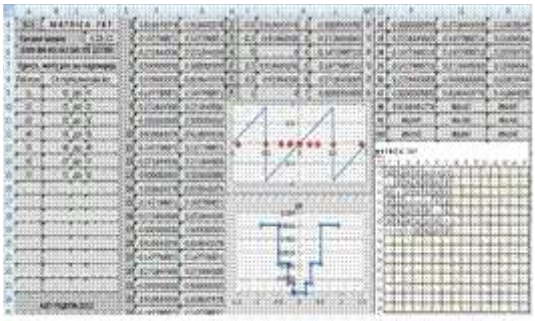

Fig. 4. Kodi në Excel për llogaritjen e matricave dhe përfaqësimi i distribucionit pdf

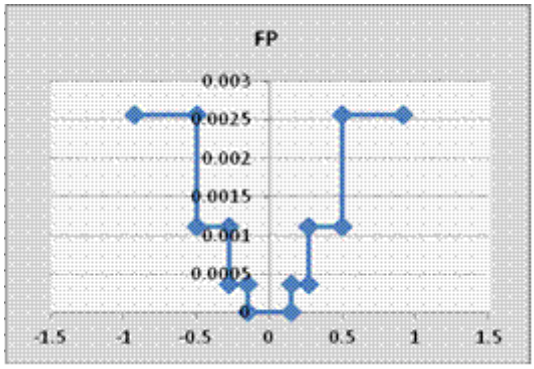

Fig. 5. Dijagrami i shpërndarjes së probabilitetit

KONKLUZIONE

Qëllimi kryesor i këtij punimi është thellimi i hulumtimeve që deri tani janë bërë në fushën e gjenerimit të numrave të rastit dhe në fushën e sistemeve kaotike-dinamike në përgjithësi dhe në fund rezulton me përmirësim të një pjese që deri tani është bërë. Pasi që është bërë një hulumtim i asaj që është punuar në këto fusha deri tani në fazën e mëvonshme të zhvillimit shkohet drejt krijimit të përmirësimeve që do rezultojnë nga puna e bërë fillimisht në MATLAB me zgjidhjen e ekuacioneve polinomiale dhe më në fund me kodin në Excel i cili me sukses llogarit probabilitet e tranzicioneve të burimeve Markov dhe me llogaritjen dhe paraqitjen grafike të shpërndarjes së probabilitetit.

BIBLIOGRAFIA

1.William Stallings: *Cryptography and Network Security Principles and Practices*, Fourth Edition; Prentice Hall, ISBN-10: 0-13-187316-4, 2005.

2.Bruce Schneier: *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code* in C; John Wiley & Sons, Inc, ISBN: 0471128457, 1996.

3.S. Callegari, R. Rovatti, and G. Setti, "Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos" *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 793 – 805, feb. 2005.

4.F. Pareschi, G. Setti, and R. Rovatti, "Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems," *IEEE Transactions on Circuits and Systems I*: Regular Papers, vol. 57, no. 12, pp. 3124 –3137, dec. 2010.

5.T. Addabbo, A. Fort, D. Papini, S. Rocchi, and V. Vignoli, "Invariant Measures of Tunable Chaotic Sources: Robustness Analysis and Efficient Estimation," *IEEE Transactions on Circuits and Systems I*, vol. 56, no. 4, pp. 806 –819, april 2009.

6.Drutarovsky, M.—Galajda, P.: Chaos–based True Random Number Generator Embedded in a mixed–signal reconfigurable hardware, *Journal of ELECTRICAL ENGINEERING*, VOL. 57, NO. 4, 2006, 218–225, 2006.

7.Mustak E. Yalcın, Johan A.K. Suykens, and Joos Vandewalle: *True Random Bit Generation from a Double Scroll Attractor*; Katholieke Universiteit Leuven Department of Electrical Engineering, ESAT-SCD-SISTA, 2004.

8.Marco Bucci and Raimondo Luzzi: *Design of Testable Random Bit Generators*; Infineon Technologies Austria AG Babenbergerstrasse 10, A-8020 Graz (AUSTRIA), 2005.

9.John Walker, Probability and Statistics.

10.Toni Stojanovski, L. Kocarev, "Chaos based random number generators Part I: *Analysis". IEEE Trans. on CAS-I*, 43(3), pp.281-288, 2001.

11.Toni Stojanovski, J. Pihl, L. Kocarev, "Chaos based random number generators Part Ⅱ: Practical realization", *IEEE Trans. on CAS-I*, vol.43(3), pp.382-385, 2001.

12.Ljupco Kocarev and Toni Stojanovski, "A Model for Secret-Key Cryptography Using Chaotic Synchronization", *Proc. of the Int. Symposium on Information Theory and Its Applications ISITA '94*, Sydney 20-24 Nov. 1994, pp. 251-255.

13.Ljupco Kocarev: Chaos-based cryptography: a brief overview, *Circuits and Systems Magazine, IEEE 1* (3), 6-21

14.Fischer, V.—Drutarovsky, M.: *True Random Number Generator Embedded in Reconfigurable Hardware*, In B.S. Kaliski Jr. et al. (Eds.): CHES 2002, LNCS 2523, Springer, Berlin, 2003, 415-430.

15.*NIST Statistical Test Suite*, http://csrc.nist.gov/rng/rng2.html

16.Devaney, R.L.: A piecewise linear model for the zones of instability of an area-preserving map, *Physica 10D*, 387-393 (1984).

17.P. Collet, J. P. Crutchfield, and J. P. Eckmann, Computing the topological entropy of maps, Comm. *Math. Phys. 88* (1983), 257-262.