2nd International Conference on

Cryptography, Network Security and Applications in the Armed Forces

Hellenic Military Academy

April 2, 2014

Abstracts

Editor: Nicholas J. Daras

Fractal Dimension as an Assessment Metric for Pseudorandom Number Generators

A.N. Veneti[1], G.C. Meletiou[2] and M.N. Vrahatis[3]

[1] Computational Intelligence Laboratory, Department of Mathematics, University of Patras, GR-26110 Patras, Greece
and
Department of Mathematics, University of Patras, GR-26110 Patras, Greece
E-mail: aveneti@upatras.gr

[2] A.T.E.I. of Epirus, P.O. 110, GR-47100 Arta, Greece,
and
University of Patras Artificial Intelligence Research Center, University of Patras, GR-26110 Patras, Greece
E-mail: gmelet@teiep.gr

[3] Computational Intelligence Laboratory, Department of Mathematics, University of Patras, GR-26110 Patras, Greece
and
Department of Mathematics, University of Patras, GR-26110 Patras, Greece
E-mail: vrahatis@math.upatras.gr

Abstract Scientific experimental results are highly dependent on the "quality" and quantity of random numbers used for these experiments. Especially in areas such as stochastic modeling and simulation, deterministic random number generators, known as pseudorandom number generators are preferred because of reproducibility of the results and their portability.

Trying to identify pseudorandom number generators which appear to be random, we examine the suitability of Fractal Dimension measurement for assessing Pseudorandom Number Generators. The established techniques that are used to evaluate a generator are focused on statistical features that are designed to detect correlations into generated random number sequences. On the other hand, Fractal Dimension is a metric that can express the randomness of the results of a pseudorandom number generator as it "quantifies" the distribution of pseudorandom numbers in Euclidean space.

We attempt to evaluate some Pseudorandom Number Generators, like classical Knuth generator, Blum-Blum-Scoob generator, the generator based on RSA cryptosystem and the generator based on the discrete logarithm problem. The computational experiments presented in our work attempt to assess the performance and the sensitivity of the examined generators. □

References

[1] Pierre L' Ecuyer: Random number generation, *Springer Berlin Heidelberg, 2012.*

[2] I. Vattulainen et al.: *A comparative study of some pseudorandom number generators*, Computer Physics Communications 86(3) (1995), pp.209-226.

[3] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone: Handbook of applied cryptography, *CRC press,* 2010.

[4] Park, Stephen K., and Keith W. Miller: *Random number generators: good ones are hard to find*, Communications of the ACM 31(10) (1988) pp.1192-1201.

[5] C. Casimir: *Not Knowing Your Random Number Generator Could Be Costly: Random Generators-Why Are They Important*, http://www.sml.ee.upatras.gr/uploadedfiles/07-rngo-!!!!!random_number_generators.pdf

[6] P. Savicky and M. Robnik-Šikonja: *Learning random numbers: A Matlab anomaly*, Applied Artificial Intelligence 22(3) (2008) pp. 254-265.

[7] C. Sevcik: *A procedure to estimate the fractal dimension of waveforms*, arXiv preprint arXiv: 1003.5266 (2010)

[8] P. D. Alevizos and M.N. Vrahatis: *Optimal Dynamic Box-Counting Algorithm*, International Journal of Bifurcation and Chaos 20(12) (2010) pp. 4067-4077