Journal of Physics: Conference Series 2017 vol.783 N1

Ternary jitter-based true random number generator

Latypov R., Stolov E.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© Published under licence by IOP Publishing Ltd. In this paper a novel family of generators producing true uniform random numbers in ternary logic is presented. The generator consists of a number of identical ternary logic combinational units connected into a ring. All the units are provided to have a random delay time, and this time is supposed to be distributed in accordance with an exponential distribution. All delays are supposed to be independent events. The theory of the generator is based on Erlang equations. The generator can be used for test production in various systems. Features of multidimensional random vectors, produced by the generator, are discussed.

http://dx.doi.org/10.1088/1742-6596/783/1/012064

References

[1] Asmussen S and Glynn P W 2007 Stochastic Simulation: Algorithms and Analysis (New York: Springer Verlag) 476
[2] Ferguson N, Schneie B and Kohno T 2010 Cryptography Engineering: Design Principles and Practical Applications (Indianapolis: Wiley) 384
[3] Horowitz P and Hill W 1980 The art of electronics (Cambridge: Cambridge University Press) 1125
[4] Petrie C S and Connelly J A 1996 Proc. IEEE Int.Symp. Circuits and Systems(Atlanta) 4 (New York: IEEE Press) A noise-based IC random number generator for applications in cryptography 324-327
[5] Golic J D 2006 New Methods for Digital Generation and Postprocessing of Random Data IEEE Trans.Comput. 55 1217-1229
[6] Sunar B, Martin W J and Stinson D R 2007 A provably secure true random number generator with built-in tolerance to active attacks IEEE Trans.Comput. 56 109-119
[7] Kuznetsov V, Pesoshin V and Stolov E 2008 Markov model of a digital stochastic generator Automation and Remote Control 69 1504-1509
[8] Wieczorek P and Golofit K 2014 Dual-Metastability Time-Competitive True Random Number Generator IEEE Trans.Circuits and Systems 61 134-145
[9] Wu X W and Prosser F P 1990 CMOS ternary logic circuits IEE Proc.Circuits, Devices and Systems 137 21-27
[10] Gaikwad V N and Deshmukh P R 2015 Design of CMOS ternary logic family based on single supply voltage 9 (New York: IEEE Press) 1-6
[11] Lisa N J and Babu H H 2015 Design of a Compact Ternary Parallel Adder/Subtractor Circuit in Quantum Computing 28 (New York: IEEE Press) 2145-2148
[12] Kleinrock L 1975 Queueing Systems: Volume I Theory (New York: Wiley-Interscience) 417
[13] Marcus M and Mink H 1964 A survey of matrix theory and matrix inequalities (Boston: Allys and Bacon) 232
[14] Bellman R 1960 Introduction to matrix analysis (New York: Macgrow-Hill) 365