Proceedings of 2018 IEEE East-West Design and Test Symposium, EWDTS 2018, 2018

A New Family of Controlled Ternary True Random Number Generators

Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2018 IEEE. Asynchronous combinational circuits with feedback containing linear units over GF(3) are considered. Using a special scheme designs one can create controlled true random generators. The offered generators can be utilized as a part of built-in security systems.

http://dx.doi.org/10.1109/EWDTS.2018.8524787

References

[1] Stipcevic M., and Koc C. K., Open Problems in Mathematics and Computational Science. Springer, 2014, ed. by Koc C. K., pp. 275-315.

[2] C. P. Sumathi, T. Santanam, and G. Umamaheswari, A Study of Various Steganographic Techniques Used for Information Hiding, Int. J. of Comp. Sc. & Eng. Survey (IJCSES), Vol. 4, No. 6, 2013, pp. 9-25.

[3] S. Sandeep, A. Singh; and S. Ghrera, A recent survey on data hiding techniques, Proc. 2017 Int. Conf. on IoT in Social, Mobile, Analytics and Cloud, 2017, pp. 882-886.

[4] V. Rozic, B. Yang, W. Dehaene, and I. Verbauwhede, Highly Efficient Entropy Extraction for True Random Number Generators on FPGAs, Proc. 52nd Design Automation Conf. (DAC), 2015, pp. 1-6.

[5] M. Dichtl, and J. Golic, High-speed true random number generation with logic gates only, In Cryptographic Hardware and Embedded Systems, ed. by P. Paillier, I. Verbauwhede (Springer, Berlin, 2007), p. 45-62.

[6] G. Stanchieri, F. Marcellis, M. Faccio, and E. Palange, An FPGA-Based Architecture of True Random Number Generator for Network Security Applications, Proc. IEEE Int. Symp. on Circuits and Systems, 2018, pp. 1-4.

[7] V. Gaudet, A survey and tutorial on contemporary aspects of multiple-valued logic and its application to microelectronic circuits. IEEE J. Emerg. Sel. Topics Circuits Syst., vol. 6, no. 1, 2016, pp. 5-12.

[8] S. Shin, E. Jang, J. Jeong, and K. Kim, CMOSCompatible Ternary Device Platform for Physical Synthesis of Multi-Valued Logic Circuits. Proc. IEEE 47th Int. Symp. on Multiple-Valued Logic, 2017, pp. 284-289.

[9] B. Cambou, P. Flikkema, J. Palmer, D. Telesca, and C. Philabaum, Can Ternary Computing Improve Information Assurance, Cryptography, vol. 2, no. 6, 2018, 16p.

[10] R. Latypov, and E. Stolov, Ternary jitter-based true random number generator, J. of Phys. : Conf. Series, vol. 783, 2017, 9p.

[11] R. Latypov, and E. Stolov, Theory of ternary jitterbased true random number generators composed of identical gates, Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki, 2017, vol. 159, no. 2, pp. 246-262.

[12] R. Latypov, and E. Stolov, Asynchronous Linear Combinational Circuits as a Base for Programmable Logic Device. Binary and Ternary Cases. IFACPapersOnLine, vol. 49, no. 26, 2016, pp. 328-383.

[13] V. Kuznetsov, V. Pesoshin, and E. Stolov, Markov model of digital stochastic generator, Automation and Remote Control, vol. 69, no. 9, 2008, pp. 1504-1509.

[14] Kemeny J. G., and Snell J. L. Finite Markov chains, Princeton, Van Nostrand, 1960.

[15] Marcus M., and Minc H. A survey of matrix theory and matrix inequalities, Allyn and Bacon, Inc., Boston, 1964.