Bernard, Florent; **Haddad, Patrick**; **Fischer, Viktor**; **Nicolai, Jean**
From physical to stochastic modeling of a TERO-based TRNG. (English) Zbl 1434.94078
J. Cryptology 32, No. 2, 435-458 (2019).

Summary: Security in random number generation for cryptography is closely related to the entropy rate at the generator output. This rate has to be evaluated using an appropriate stochastic model. The stochastic model proposed in this paper is dedicated to the transition effect ring oscillator (TERO)-based true random number generator (TRNG) proposed by *M. Varchola* and *M. Drutarovsky* [CHES 2010, Lect. Notes Comput. Sci. 6225, 351–365 (2010; Zbl 1434.94079). The advantage and originality of this model are that it is derived from a physical model based on a detailed study and on the precise electrical description of the noisy physical phenomena that contribute to the generation of random numbers. We compare the proposed electrical description with data generated in two different technologies: TERO TRNG implementations in 40 and 28 nm CMOS ASICs. Our experimental results are in very good agreement with those obtained with both the physical model of TERO's noisy behavior and the stochastic model of the TERO TRNG, which we also confirmed using the AIS 31 test suites.

MSC:

94A62 Authentication, digital signatures and secret sharing
94A17 Measures of information, entropy

Keywords:

hardware random number generators; transition effect ring oscillator (TERO); stochastic models; entropy; statistical tests

Software:

Diehard; NIST Statistical Test Suite

Full Text: DOI

References:

[1] Baudet, M.; Lubicz, D.; Micolod, J.; Tassiaux, A., On the security of oscillator-based random number generators, J. Cryptol., 24, 398-425, (2011) · Zbl 1251.94021

[2] Bernard, F.; Fischer, V.; Valtchanov, B., Mathematical model of physical RNGs based on coherent sampling, Tatra Mt. Math. Publ., 45, 1-14, (2010) · Zbl 1274.94041

[3] V. Fischer, A closer look at security in random number generators design, in \textit{Constructive Side-Channel Analysis and Secure Design—COSADE 2012} (Springer, 2012), pp. 167-182

[4] P. Haddad, Y. Teglia, F. Bernard, V. Fischer, On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models, in \textit{Proceedings of Design, Automation and Test in Europe DATE 2014} (Dresden, Germany, March 2014), pp. 1-6

[5] L. Hars, Random number generation based on oscillatory metastability in ring circuits. https://eprint.iacr.org/2011/637.pdf (2011)

[6] W. Killmann, W. Schindler, A design for a physical RNG with robust entropy estimators, in Elisabeth Oswald and Pankaj Rohatgi, editors, \textit{Cryptographic Hardware and Embedded Systems—CHES 2008, volume 5154 of LNCS} (Springer, 2008), pp. 146-163

[7] W. Killmann, W. Schindler, A proposal for: functionality classes for random number generators. https://www.bsi.bund.de (2011)

[8] G. Marsaglia, DIEHARD: Battery of Tests of Randomness. http://stat.fsu.edu/pub/diehard/ (1996)

[9] Reyneri, LM; Corso, D.; Sacco, B., Oscillatory metastability in homogeneous and inhomogeneous flip-flops, IEEE J. Solid-State Circuits, 25, 254-264, (1990)

[10] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications—NIST SP 800-22, rev. 1a (2010)

[11] C. Shannon, A mathematical theory of communication. \textit{Bell Syst. Tech. J.}\textbf{27}, 379-423, 623-656 July, (1948)

· Zbl 1154.94303

[12] B. Sunar, W.J. Martin, D.R. Stinson, A provably secure true random number generator with built-in tolerance to active attacks. \textit{IEEE Trans. Comput.} 109-119 (2007) · Zbl 1391.94799

[13] M. Varchola, M. Drutarovsky, New high entropy element for FPGA based true random number generators, in \textit{Cryptographic Hardware and Embedded Systems (CHES), 2010} (Springer, 2010), pp. 351-365