Ma, Yuan; **Lin, Jingqiang**; **Jing, Jiwu**

On the entropy of oscillator-based true random number generators. (English) Zbl 1383.94031

Handschuh, Helena (ed.), Topics in cryptology – CT-RSA 2017. The cryptographers' track at the RSA conference 2017, San Francisco, CA, USA, February 14–17, 2017. Proceedings. Cham: Springer (ISBN 978-3-319-52152-7/pbk; 978-3-319-52153-4/ebook). Lecture Notes in Computer Science 10159, 165-180 (2017).

Summary: True random number generators (TRNGs) are essential for cryptographic systems, and they are usually evaluated by the concept of entropy. In general, the entropy of a TRNG is estimated from its stochastic model, and reflected in the statistical results of the generated raw bits. Oscillator-based TRNGs are widely used in practical cryptographic systems due to its elegant structure, and its stochastic model has been studied in different aspects. In this paper, we investigate the applicability of the different entropy estimation methods for oscillator-based TRNGs, including the bit-rate entropy, the lower bound and the approximate entropy. Particularly, we firstly analyze the two existing stochastic models (one of which is phase-based and the other is time-based), and deduce consistent bit-rate entropy results from these two models. Then, we design an approximate entropy calculation method on the output raw bits of a simulated oscillator-based TRNG, and this statistical calculation result well matches the bit-rate entropy from stochastic models. In addition, we discuss the extreme case of tiny randomness where some methods are inapplicable, and provide the recommendations for these entropy evaluation methods. Finally, we design a hardware verification method in a real oscillator-based TRNG, and validate these estimation methods in the hardware platform.

For the entire collection see [Zbl 1356.94003].

MSC:

94A60 Cryptography
65C10 Random number generation in numerical analysis

Keywords:

oscillators; true random number generators; entropy estimation; stochastic model

Software:

Diehard; NIST Statistical Test Suite

Full Text: DOI

References:

[1] Amaki, T., Hashimoto, M., Mitsuyama, Y., Onoye, T.: A worst-case-aware design methodology for noise-tolerant oscillator-based true random number generator with stochastic behavior modeling. IEEE Trans. Inf. Forensics Secur. 8(8), 1331–1342 (2013) · doi:10.1109/TIFS.2013.2271423

[2] Baudet, M., Lubicz, D., Micolod, J., Tassiaux, A.: On the security of oscillator-based random number generators. J. Cryptol. 24(2), 398–425 (2011) · Zbl 1251.94021 · doi:10.1007/s00145-010-9089-3

[3] Box, G.E.P., Jenkins, G.: Time Series Analysis: Forecasting and Control, pp. 28–32. Holden-Day, San Francisco (1976) · Zbl 0363.62069

[4] Fischer, V., Lubicz, D.: Embedded evaluation of randomness in oscillator based elementary TRNG. In: Batina, L., Robshaw, M. (eds.) CHES 2014. LNCS, vol. 8731, pp. 527–543. Springer, Heidelberg (2014). doi: 10.1007/978-3-662-44709-3_29 · Zbl 06461372 · doi:10.1007/978-3-662-44709-3_29

[5] Haddad, P., Teglia, Y., Bernard, F., Fischer, V.: On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models. In: IEEE Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 1–6 (2014)

[6] Information Technology Laboratory: FIPS 140-2: Security Requirement For Cryptographic Modules (2011)

[7] ISO/IEC 18031: Information Technology - Security Techniques - Random bit generation (2011)

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

[9] Killmann, W., Schindler, W.: A design for a physical RNG with robust entropy estimators. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 146–163. Springer, Heidelberg (2008). doi: 10.1007/978-3-540-85053-3_10 · Zbl 05488428 · doi:10.1007/978-3-540-85053-3_10

[10] Ma, Y., Lin, J., Chen, T., Xu, C., Liu, Z., Jing, J.: Entropy evaluation for oscillator-based true random number generators. In: Batina, L., Robshaw, M. (eds.) CHES 2014. LNCS, vol. 8731, pp. 544–561. Springer, Heidelberg (2014). doi: 10.1007/978-3-662-44709-3_30 · Zbl 06461373 · doi:10.1007/978-3-662-44709-3_30

[11] Marsaglia, G.: Diehard Battery of Tests of Randomness. http://www.stat.fsu.edu/pub/diehard/

[12] Menezes, A., Oorschot, P.V., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1997) · Zbl 0868.94001

[13] Rukhin, A., et al.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800–22. http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/Spp800-22rev1a.pdf

[14] Valtchanov, B., Fischer, V., Aubert, A., Bernard, F.: Characterization of randomness sources in ring oscillator-based true random number generators in FPGAs. In: DDECS, pp. 48–53 (2010) · doi:10.1109/DDECS.2010.5491819