Shen, Jiahui; **Chen, Tianyu**; **Wang, Lei**; **Ma, Yuan**

An efficiency optimization scheme for the on-the-fly statistical randomness test. (English)
Zbl 1452.94083
Qing, Sihan (ed.) et al., Information and communications security. 19th international conference, ICICS 2017, Beijing, China, December 6–8, 2017. Proceedings. Cham: Springer. Lect. Notes Comput. Sci. 10631, 17-35 (2018).

Summary: In many cryptographic systems, random number can significantly influence its security. Although in practice random number generators (RNGs) are allowed to adopt only after strict analysis and security evaluation, the environmental factors also may lead the randomness of generated sequences to degrade. Therefore, on-the-fly statistical randomness test should be used to evaluate a candidate random sequence. Unfortunately, existing randomness test methods, such as the NIST test suite, are not well suitable to directly serve as on-the-fly test, because timely execution is usually not considered in their designs. In this paper, we propose a scheme to optimize the efficiency of randomness test suites, that is, providing the optimized order of the tests in a test suite, so that an unqualified sequence can be rejected as early as possible. This scheme finds out the optimized order by balancing the coverage, independence and time consumption of each test, and minimizing the average elimination time. We apply this optimization scheme on the revised NIST test suite as an instance. Experimental results on the sequences of 128 and 256 bits, demonstrate that the optimized efficiency approximates to the theoretical optimum and the scheme can be quickly implemented.

For the entire collection see [Zbl 1435.68039].

MSC:

94A60 Cryptography

Keywords:

on-the-fly statistical randomness test; efficiency optimization; execution order; average elimination time used; multi-attribute weight allocation

Software:

Diehard; TestU01

Full Text: DOI

References:

[1] Vasyltsov, I., Hambardzumyan, E., Kim, Y.-S., Karpinskyy, B.: Fast digital TRNG based on metastable ring oscillator. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 164-180. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85053-3_11

[2] Markettos, A.T., Moore, S.W.: The frequency injection attack on ring-oscillator-based true random number generators. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 317-331. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04138-9_23

[3] Fischer, V., Aubert, A., Bernard, F., et al.: True Random Number Generators in Configurable Logic Devices. Project ANR-ICTeR (2009)

[4] Schindler, W.: Efficient online tests for true random number generators. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 103-117. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44709-1_10 · Zbl 1006.68704

[5] Rukhin, A., Soto, J., Nechvatal, J., et al.: A statistical suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22, Washington, D.C., May 2001

[6] Sönmez Turan, M., DoĞanaksoy, A., Boztaş, S.: On independence and sensitivity of statistical randomness tests. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 18-29. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85912-3_2 · Zbl 1198.65030

[7] NIST FIPS PUB: 140-2: Security Requirements for Cryptographic Modules. Washington, D.C., USA (2001)

[8] Elaine, B., John, K.: Recommendation for random number generation using deterministic random bit generators. NIST Special

Publication 800-90A, Washington, D.C., January 2012

[9] Killmann, W., Schindler, W.: AIS 31: Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators. Version 3.1. T-Systems GEI GmbH and Bundesamt fr Sicherheit in der Informationstechnik (BSI), Bonn, Germany (2001)

[10] Marsaglia, G.: The Marsaglia Random Number CDROM Including the Diehard Battery of Tests of Randomness (1995)

[11] L'Ecuyer, P., Simard, R.J.: TestU01: AC library for empirical testing of random number generators. ACM Trans. Math. Softw. 33(4) (2007) · Zbl 1365.65008

[12] L'Ecuyer, P.: Testing random number generators. In: Winter Simulation Conference, pp. 305-313. ACM Press (1992)

[13] Hellekalek, P., Wegenkittl, S.: Empirical evidence concerning AES. ACM Trans. Model. Comput. Simul. 13(4), 322-333 (2003)

[14] Fan, L., Chen, H., Gao, S.: A general method to evaluate the correlation of randomness tests. In: Kim, Y., Lee, H., Perrig, A. (eds.) WISA 2013. LNCS, vol. 8267, pp. 52-62. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-05149-9_4

[15] Maurer, U.M.: A universal statistical test for random bit generators. J. Cryptol. 5(2), 89-105 (1992) · Zbl 0790.94014

[16] Hamano, K., Kaneko, T.: Correction of overlapping template matching test included in NIST randomness test suite. IEICE Trans. 90-A(9), 1788-1792 (2007)

[17] Kim, S.-J., Umeno, K., Hasegawa, A.: Corrections of the NIST statistical test suite for randomness. IACR Cryptology ePrint Archive 2014:18-31 (2004)

[18] Hamano, K.: The distribution of the spectrum for the discrete fourier transform test included in SP800-22. IEICE Trans. 88-A(1), 67-73 (2005)

[19] Pareschi, F., Rovatti, R., Setti, G.: On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. IEEE Trans. Inf. Forensics Secur. 7(2), 491-505 (2012)

[20] Sulak, F., Doğanaksoy, A., Ege, B., Koçak, O.: Evaluation of randomness test results for short sequences. In: Carlet, C., Pott, A. (eds.) SETA 2010. LNCS, vol. 6338, pp. 309-319. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-15874-2_27 · Zbl 1257.62128

[21] Suciu, A., Nagy, I., Marton, K., Pinca, I.: Parallel implementation of the NIST statistical test suite. In: Proceedings of the 2010 IEEE 6th International Conference on Intelligent Computer Communication and Processing (ICCP), pp. 363-368. Institute of Electrical and Electronic Engineers (2010)

[22] Huang, J., Lai, X.: Measuring random tests by conditional entropy and optimal execution order. In: Chen, L., Yung, M. (eds.) INTRUST 2010. LNCS, vol. 6802, pp. 148-159. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25283-9_10

[23] Chen, T., Ma, Y., Lin, J., Wang, Z., Jing, J.: An efficiency optimization scheme for the on-the-fly statistical randomness test. In: Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud), CSCLOUD 2015, pp. 515-517. IEEE Computer Society, Washington, D.C. (2015)

[24] Soto, J.: Statistical testing of random number generators. In: Proceedings of the 22nd National Information Systems Security Conference (NISSC), vol. 10, pp. 12-23. NIST, Gaithersburg (1999)

[25] Soto, J.: Randomness Testing of the AES Candidate Algorithms. NIST (1999). csrc.nist.gov

[26] NIST: The NIST Statistical Test Suite (2010). http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.1.2.zip · Zbl 1271.65013

[27] Chen, C. · Zbl 1134.94337