Sulak, Fatih; **Doğanaksoy, Ali**; **Ege, Barış**; **Koçak, Onur**

Evaluation of randomness test results for short sequences. (English) Zbl 1257.62128

Carlet, Claude (ed.) et al., Sequences and their applications – SETA 2010. 6th international conference, Paris, France, September 13–17, 2010. Proceedings. Berlin: Springer (ISBN 978-3-642-15873-5/pbk). Lecture Notes in Computer Science 6338, 309-319 (2010).

Summary: Randomness testing of cryptographic algorithms are of crucial importance to both designer and the attacker. When block ciphers and hash functions are considered, the sequences subject to randomness testing are of at most 512-bit length, "short sequences". As it is widely known, NIST has a statistical test suite to analyze the randomness properties of sequences and generators. However, some tests in this suite can not be applied to short sequences and most of the remaining ones do not produce reliable test values for the sequences in question. Consequently, the analysis method which is proposed in this suite is not suitable for evaluation of generators which produce relatively short sequences. We propose an alternative approach to analyze short sequences without tweaking the tests.

For the entire collection see [Zbl 1194.94017].

MSC:

62P99 Applications of statistics
94A60 Cryptography
62F99 Parametric inference
62-04 Software, source code, etc. for problems pertaining to statistics

Full Text: DOI