УДК 004.9

М.В. Некрасова, канд. техн. наук, доц., НТУ «ХПІ»

МЕТОДИ ТЕСТУВАННЯ ГЕНЕРАТОРІВ ВИПАДКОВИХ І ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У статті розглянуті існуючі методи оцінки якості випадкових послідовностей біт. Описані пакети статистичних тестів. За допомогою системи статистичних тестів NIST проведено дослідження статистичних властивостей сформованих розробленими генераторами псевдовипадкових послідовностей та проведено їх перевірку на випадковість за допомогою порівняння зі статистикою ідеально випадкового ряду. За результатами дослідження обрано пороговий рівень проходження тестів NIST та вироблено інженерні рекомендації щодо вибору генератора псевдовипадкових чисел з найбільшою кількістю успішно пройдених тестів. Для стендів напівнатурного моделювання асинхронних радіоелектронних систем рекомендується застосування генератора псевдовипадкових чисел на основі методу Мерсенна Твістера. Також встановлено необхідність удосконалення розроблених генераторів шляхом підбору вхідних параметрів з метою підвищення ймовірності проходження тестів.

Ключові слова: генератори випадкових послідовностей, послідовність біт, псевдовипадкова послідовність, статистичні тести, статистичні тести NIST, випадковість, методи моделювання.

The article reviews existing methods for assessing the quality of random bit sequences. Statistical test suites are described. Using the NIST statistical test system, the statistical properties of sequences generated by the developed pseudorandom sequence generators were investigated, and their randomness was verified by comparing them with the statistics of an ideally random sequence. Based on the study results, a threshold level for passing the NIST tests was selected, and engineering recommendations were developed for choosing a pseudorandom number generator with the highest number of successfully passed tests. For hardware-in-the-loop modeling stands of asynchronous radio-electronic systems, it is recommended to use a pseudorandom number generator based on the Mersenne Twister method. The study also identified the need to improve the developed generators by selecting input parameters to increase the probability of passing the tests.

Keywords: random sequence generators, bit sequence, pseudorandom sequence, statistical tests, NIST statistical tests, randomness, modeling methods.

Список літератури

1. Random Number Generators: An Evaluation and Comparison of Random.org and SomeCommonly Used Generators. Режим доступу: https://www.random.org/analysis/Analysis2005.pdf
2. Security Requirements For Cryptographic Modules. Режим доступу: *http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf*
3. Brown R. Dieharder: A Random Number Test Suite. Режим доступа: http://www.phy.duke.edu/~rgb/General/dieharder.php
4. A statistical test suite for random and pseudorandom number generators for cryptographic application / A. Rukhin, J. Soto, J. Nechvatal et al. // NIST Special Publication. 800-22 Revision la. Gaithersburgational Institute of Standards and Technology, 2010. 131 p.
5. Recommendation for the Entropy Sources Used for Random Bit Generation. Режим доступу: http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf
6. Recommendation for Random Bit Generator (RBG) Constructions. Режим доступу: http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90c.pdf
7. Maksymovych, V., Shevchuk, M., & Mandrona, M. (2016). *Research of pseudorandom bit sequence generators based on LFSR*. Lviv Polytechnic National University. https://ena.lpnu.ua/items/215c5cc2-816a-4a46-89db-259eb7ae3be3
8. Poluyanenko, N. (2017). *Development of the search method for nonlinear shift registers using hardware, implemented on field programmable gate arrays*. European Journal of Engineering, 5(3), 45–53. https://journal.eu-jr.eu/engineering/article/view/271
9. Zhang, X.-F., & Fan, J.-L. (2010). *Pseudo-random sequence generating method based on LFSR and chaotic system*. Acta Physica Sinica, 59(3), 2289–2295. https://wulixb.iphy.ac.cn/en/article/doi/10.7498/aps.59.2289
10. I. M., et al. (2020). *Pseudorandom number generator (PRNG) design using hyper-chaotic modified robust logistic map (HC-MRLM)*. Electronics, 9(1), 104. https://www.mdpi.com/2079-9292/9/1/104
11. Nguyen, N. T., & Bui, T. Q., et al. (2021). *Designing a pseudo-random bit generator with a novel 5D-hyperchaotic system*. arXiv. https://arxiv.org/abs/2105.08896
12. Kushnir, M. Ya., Kosovan, H. V., & Kroyalo, P. M. (2022). *Properties of generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems*. Research in Cybernetics, 18(2), 112–125. https://ric.zp.edu.ua/article/view/254427

References (transliterated)

1. Random Number Generators: An Evaluation and Comparison of Random.org and SomeCommonly Used Generators. Режим доступу: https://www.random.org/analysis/Analysis2005.pdf
2. Security Requirements For Cryptographic Modules. Режим доступу: *http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf*
3. Brown R. Dieharder: A Random Number Test Suite. Режим доступа: http://www.phy.duke.edu/~rgb/General/dieharder.php
4. A statistical test suite for random and pseudorandom number generators for cryptographic application / A. Rukhin, J. Soto, J. Nechvatal et al. // NIST Special Publication. 800-22 Revision la. Gaithersburgational Institute of Standards and Technology, 2010. 131 p.
5. Recommendation for the Entropy Sources Used for Random Bit Generation. Режим доступу: http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf
6. Recommendation for Random Bit Generator (RBG) Constructions. Режим доступу: http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90c.pdf
7. Maksymovych, V., Shevchuk, M., & Mandrona, M. (2016). *Research of pseudorandom bit sequence generators based on LFSR*. Lviv Polytechnic National University. https://ena.lpnu.ua/items/215c5cc2-816a-4a46-89db-259eb7ae3be3
8. Poluyanenko, N. (2017). *Development of the search method for nonlinear shift registers using hardware, implemented on field programmable gate arrays*. European Journal of Engineering, 5(3), 45–53. https://journal.eu-jr.eu/engineering/article/view/271
9. Zhang, X.-F., & Fan, J.-L. (2010). *Pseudo-random sequence generating method based on LFSR and chaotic system*. Acta Physica Sinica, 59(3), 2289–2295. https://wulixb.iphy.ac.cn/en/article/doi/10.7498/aps.59.2289
10. I. M., et al. (2020). *Pseudorandom number generator (PRNG) design using hyper-chaotic modified robust logistic map (HC-MRLM)*. Electronics, 9(1), 104. https://www.mdpi.com/2079-9292/9/1/104
11. Nguyen, N. T., & Bui, T. Q., et al. (2021). *Designing a pseudo-random bit generator with a novel 5D-hyperchaotic system*. arXiv. https://arxiv.org/abs/2105.08896
12. Kushnir, M. Ya., Kosovan, H. V., & Kroyalo, P. M. (2022). *Properties of generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems*. Research in Cybernetics, 18(2), 112–125. https://ric.zp.edu.ua/article/view/254427

Відомості про авторів/ About the Authors

Некрасова Марія Володимирівна – кандидат технічних наук, доцент, Національний технічний університет «Харківський політехнічний інститут»; тел.: (057)-707-64-54; e-mail: masha12dec@gmail.com

Nekrasova Mariia Volodymyrivna – Candidate of Technical Sciences, Dozent, National Technical University "Kharkiv Polytechnic Institute"; tel.: (057)-707-60-58; e-mail: masha12dec@gmail.com