



2022

COMPUTER DATA ANALYSIS AND MODELING:

STOCHASTICS AND DATA SCIENCE

Proceedings
of the XIII International Conference

Minsk, September 6–10, 2022



M&I

Maltsev M.V., Kharin Yu.S. On testing randomness using frequency estimators	112
Malugin V.I., Kornievich A.K. Multi-country analysis of the COVID-19 pandemic typology using machine learning algorithms	116
Marshalova A.E., Bruches E.P., Batura T.V. Aspect extraction from scientific texts	122
Mukha V.S., Kako N.F. On the dual stabilization of the multidimensional regression object at a given level	126
Musaev A.A., Grigoriev D.A. Analysis of chaotic process forecast effectiveness based on terminal indicators of management quality	131
Nysanbayeva S.E., Kapalova N.A., Dyusenbayev D.S., Algazy K.T., Sakan K.S. Investigation of the statistical security of a pseudo-random sequence generator	137
Palamarchuk E.S. On robustness of the optimal feedback law in a stochastic linear-quadratic control problem under cost uncertainty	144
Palukha U.Yu., Kharin Yu.S., Siarheeu A.I., Arlou A.A. On statistical testing of random and pseudorandom sequences based on entropy functionals	148
Pirshtuk I.K., Serikova N.V. On statistical evaluation of randomness based on minimum entropy estimator	163
Piterbarg V.I., Alieva P.N. On large excursions probabilities for Gaussian copula vector processes. Applications in reliability and finance	168
Pranevich A.F., Khatskevich G.A. Dynamic three-factor production functions with hicks-neutral technological progress	172
Savelov M.P. The limiting distributions of statistics of several criteria from the NIST statistical test suite	176
Sharilova E. Statistical assessment of the real demographic security of the Republic of Belarus	180
Sokolova M.V., Romanova O.N., Kolomiets N.D., Bosiakov S.M. Forecasting cases of children disease by non-invasive forms of pneumococcal infection	184
Soshnikova L.A. Using the logistic regression in analysis of results from statistical observations	187
Spesivtsev A.V., Mikhailov V.V. The fuzzy-possibility approach to overcoming complexity under uncertainty	192
Trutschnig W. Quantifying and estimating (multivariate) directed dependence	196
Tsirul E.A., Badziahin I.A. Modifications of the imputation method for parameter estimation of censored autoregressive time series	202
Vana L., Visconti E., Nenzi L., Cadonna A., Kastner G., Parzer R. Posterior predictive model checking using formal methods	205

INVESTIGATION OF THE STATISTICAL SECURITY OF A PSEUDO-RANDOM SEQUENCE GENERATOR

S.E. NYSANBAYEVA¹, N.A. KAPALOVA², D.S. DYUSENBAYEV³, K.T. ALGAZY⁴,
K.S. SAKAN⁵

*Institute of Information and Computational Technologies of the RK MES
Laboratory of Information Security
Almaty, KAZAKHSTAN*

e-mail: ¹sultasha1@mail.ru, ²kapalova@ipic.kz, ³dimash_dds@mail.ru,
⁴kunbolat@mail.ru, ⁵kairat_sks@mail.ru

The paper considers a pseudo-random sequence generator built on a multiplicative operation and implemented to test its security. The statistical properties of the sequences generated using this generator are investigated. The results of the analysis of the statistical characteristics of the generated sequences obtained by statistical tests from the D. Knuth and NIST-822 STS sets are presented.

Keywords: data science, pseudo-random generator, statistical security

1 Introduction

Pseudorandom sequence (PRS) generators are an essential element of any security system. By a pseudo-random sequence, we mean a sequence obtained using a deterministic algorithm. The sequence generated by the deterministic algorithm is not random. One can make sure that the sequence of numbers is random either with the help of statistical tests that reveal the specific features of random sequences or by analytical and computational methods [1]. It is on their properties that the reliability and security of the processes of collecting, processing, transmitting, and storing information, as well as managing objects depend. In this regard, the most stringent requirements are imposed on the generated sequences.

A high-quality PRS generator intended for use in information security systems should meet the following requirements [2]:

- To be cryptographically strong;
- To have good statistical properties, a PRS in its statistical properties should not differ from a truly random sequence;
- To have a large period of the generated sequence, for example, when ciphering, for the transformation of each element of the input sequence, it is necessary to use a separate element of the pseudo-random sequence;
- Efficient hardware and software implementations are possible.

The following assertion is also true: a PRS generator unpredictable to the left is cryptographically secure. A cryptanalyst who knows the principle of operation of such