2022

COMPUTER DATA ANALYSIS AND MODELING:

STOCHASTICS AND DATA SCIENCE

Proceedings
of the XIII International Conference

Minsk, September 6–10, 2022

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

S.E. Nysanbayeva[1], N.A. Kapalova[2], D.S. Dyusenbayev[3], K.T. Algazy[4], K.S. Sakan[5]

Institute of Information and Computational Technologies of the RK MES
Laboratory of Information Security
Almaty, KAZAKHSTAN
e-mail: [1]sultasha1@mail.ru, [2]kapalova@ipic.kz, [3]dimash_dds@mail.ru,
[4]kunbolat@mail.ru, [5]kairat_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