Ann. Acad. Rom. Sci.
Ser. Math. Appl.
ISSN 2066-6594 Vol. 12, No. 1-2/2020

SELF-SHRINKING CHAOS BASED PSEUDO-RANDOM ALGORITHM*

Borislav Stoyanov†

DOI https://doi.org/10.56082/annalsarscimath.2020.1-2.246

Dedicated to Dr. Vasile Drăgan on the occasion of his 70th anniversary

Abstract

We propose a novel self-shrinking chaos based pseudo-random number output algorithm. The result of the analysis shows that the presented generator ensures a secure way for sending electronic information with critical applications in data encryption.
MSC: 41A50, 11K45, 11B83

keywords: Chebyshev polynomial, self-shrinking rule, pseudo-random byte generator, statistical suite.

1 Introduction

Random number generators are physical sources (atmospheric noise, electrical noise, radioactive decay, etc.) that return uniformly distributed and completely unpredictable values. Truly random numbers are applicable for a kind of tasks, such as encrypting data, gaming, and experimental design. Generating random numbers is particularly hard. Pseudo-random generators are software alternative algorithms to truly random generators. They

*Accepted for publication on April 21, 2020

†borislav.stoyanov@shu.bg University of Shumen, Bulgaria; Paper written is partially supported of the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science.