

Statistical properties of random sequences produced by chaotic dynamical systems: Cryptographic point of view

Dmytro D. Vavriv^{*}, Klaus Schuenemann

Technical University Hamburg-Harburg, High Frequency Technology Institut,
Denickestr 22(I), D-21073 Hamburg, Germany

^{*} Electronic Address: vavriv@ukrpost.net

The paper describes a possibility of using deterministic nonlinear dynamical systems with chaotic behavior as generators of random sequences. Statistical characteristics of binary sequences produced by a random generator on the basis of the Mackey-Glass equation have been analyzed. It has been shown that in some areas of the control parameters, these sequences pass the standard cryptographic tests specified by US Standard FIPS PUB 140-1/140-2. The obtained results indicate that the formation of binary random sequences by using deterministic dynamical systems with chaotic behavior is promising for cryptographic applications.

by masking without synchronization”, by physiological control systems”,