IEEE International Black Seas Conference on Communications and Networking (BlackSeaCom)
Article number 11598257, 2026, Pages 1–6

Cryptographically Resilient Random Number Generators based on Entropy Sources in Information Security Systems

Kostiuk, Y.[a], Sokolov, V.[a], Skladannyi, P.[a], Kuzminykh, I.[b], Ghita, B.[c]

[a] Borys Grinchenko Kyiv University, Kyiv, Ukraine
[b] King's College London, Department of Informatics, London, United Kingdom
[c] University of Plymouth, School of Computing and Mathematics, Plymouth, United Kingdom

Abstract

The paper proposes a hybrid entropy-controlled random number generator for information security systems that combines physical entropy sources, cryptographic conditioning, and adaptive feedback control. A comparative analysis of traditional pseudo-random and quantum generators was conducted, and experimental testing was performed in accordance with NIST SP 800-90B, NIST SP 800-90C, and ISO/IEC 18031:2025. According to statistical analysis of a large volume of bit sequences, minimum entropy close to unity was observed, with only a slight deviation, confirming the high randomness. The throughput of the hardware implementation is ~ 600 Mbit/s (over 500 Mbit/s) with an energy consumption of E ≈ 0.29 mJ/Mbit. Compared to classical generators on an uncontrolled cypher counter or hardware generators on ring oscillators without pre-mixing, a reduction in correlation and mean shift of more than a third has been achieved. The proposed architecture demonstrates resistance to source manipulation, fault injection, and side-channel attacks, confirming the effectiveness of the entropy approach for modern cryptographic systems, Internet of Things platforms, and security modules.

Author keywords

cryptographic resistance; entropy sources; hybrid generation; random number generators; stochastic modelling

About this paper

https://ieeexplore.ieee.org/document/11598257
DOI: 10.1109/BlackSeaCom69760.2026.11598257

Online ISBN: 979-8-3195-4344-8
Online ISSN: 2687-9808
EID: 2-s2.0-105045588708

First Online: 13 July 2026
Original language: English
Publisher: IEEE Inc.