Document details

‹ Back to results | 1 of 1

CSV export Download Print E-mail Save to PDF Save to list More...

Full Text View at Publisher

Proceedings - International Conference on Intelligent Systems, Modelling and Simulation, ISMS
Volume 2015-September, 28 September 2015, Article number 7281012, Pages 772-774
5th International Conference on Intelligent Systems, Modelling and Simulation, ISMS 2014; Langkawi; Malaysia; 27 January 2014 through 29 January 2014; Category numberE3857; Code 117206

Randomness analysis of pseudo random noise generator using 24-Bits LFSR (Conference Paper)

Hazwani, S., Khan, S., Siddiqi, M.U., Al-Khateeb, K.A.S., Habaebi, M.H., Shahid, Z.

Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM), Malaysia

Abstract

View references (10)

We have described in previous work the generation of PN-sequence by employing a 4-bit shifted Linear Feedback Shift Register (LFSR) for application into Direct Sequence Spread Spectrum (DSSS) system by simulation. In this paper, is proposed a pseudo random number generator (PRNG) circuit consisting of 24-bit shift registers (LFSR) which has much longer period to improve statistical properties. We simulated the LFSR circuit by using Multisim 11.0 and the pseudo random sequence generated is tested with statistical test of NIST Test suite. The sequence is passed the entire selected test and we concluded that our pseudo random sequence has long enough period to be considered as random. © 2014 IEEE.

Author keywords

Linear feedback shift register (LFSR) | NIST SP800-22 | Pseudo random number generator (PRNG) | Pseudo random sequence | Randomness tests

Indexed keywords

Engineering controlled terms: Intelligent systems | Number theory | Random number generation | Random processes | Reconfigurable hardware

Linear feedback shift registers | Pseudo random number generators | Pseudorandom sequences | Randomness test | SP800-22

Engineering main heading: Shift registers

ISSN: 21660662
ISBN: 978-1479993857-5
Source Type: Conference Proceeding
Original language: English

DOI: 10.1109/ISMS.2014.141
Document Type: Conference Paper
Volume Editors: Al-Dabass D., Sauli Z., Zakaria Z.
Sponsors:
Publisher: IEEE Computer Society

References (10)

View in search results format ›

All | CSV export | Print | E-mail | Save to PDF | Create bibliography

1 Massodi, F., Alam, S., Bukhori, M.U.
An analysis of linear feedback shift registers in stream chippers
International Journal of Applications (0975-8887), 46 (17), pp. 46-49.
May 2012