Chapter 3

Pseudorandom Number Generators Based on Cellular Automata

ABSTRACT

In this chapter, the author considers the main theoretical solutions for the creation of pseudo-random number generators based on one-dimensional cellular automata. A Wolfram generator is described on the basis of rule 30. The main characteristics of the Wolfram generator is presented. The analysis of hybrid pseudo-random number generators based on cellular automata is carried out. Models of such generators and their realization with various forms of neighborhoods are presented. Also in the chapter is presented the analysis of the basic structures and characteristics of pseudo-random number generators using additional sources of pseudo-random numbers. As such additional sources the LFSR is used.

THE GENERATORS BASED ON ONE-DIMENSIONAL CELLULAR AUTOMATA: WOLFRAM GENERATOR

In PRNG based on one-dimensional CA the elementary cellular automata is used. One of the rules is selected and the evolution of the elementary cellular automata on the basis of this rule is studied. In addition, elementary cellular automata in the initial state is set. The signals are generated at the elementary cellular automata cell outputs in each subsequent time step and their values

DOI: 10.4018/978-1-5225-2773-2.ch003
Pseudorandom Number Generators Based on Cellular Automata


First PRNG based on the elementary cellular automata was proposed by S. Wolfram and he detailed studied its properties (Wolfram, 1986a, 1986b). S. Wolfram studied the many rules and selected generators, which are similar to the LFSR.

Based rule 30 generator generates a good random sequence.

\[ X_i(t + 1) = X_{i-1}(t) \oplus [X_i(t) \lor X_{i+1}(t)]. \]

The CA evolution by rule 30 is shown on Figure 1.

The generator on the basis of this rule has been investigated in papers (Wolfram, 1986a, 1986b, 1985). In the works is defined class of the rules that are making the elementary cellular automata by similar to the LFSR. These rules use the modulo k function. Most often k=2 is used, In this case, a function is called haw the XOR function. PRNG based on elementary cellular automata was investigated for characteristics such as length of repeat period, spatial and temporal distribution characteristics of elementary cellular automata states and size of elementary cellular automata.

Pseudorandom number generator based on one-dimensional CA have been widely studied in the works (Cattel, Zang, Serra, & Muzio, 1999; Chowdhury, Nandy, & Chattopadhyay, 1994; Sipper, 1999; Bhattacharjee, Paul, & Das, 2016; Cardell & Fúster-Sabater, 2016; Sirakoulis, 2016; Spencer, 2015). Much

Figure 1. An example of the elementary cellular automata evolution based on the rule 30
12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage: www.igi-global.com/chapter/pseudorandom-number-generators-based-on-cellular-automata/190213?camid=4v1


Related Content

A Partial Optimization Approach for Privacy Preserving Frequent Itemset Mining
Shibnath Mukherjee, Aryya Gangopadhyay and Zhiyuan Chen (2010). International Journal of Computational Models and Algorithms in Medicine (pp. 19-33). www.igi-global.com/article/partial-optimization-approach-privacy-preserving/38942?camid=4v1a

Test Suite Optimization Using Chaotic Firefly Algorithm in Software Testing
Evolutionary Approaches for the Extraction of Classification Rules
[www.igi-global.com/article/evolutionary-approaches-for-the-extraction-of-classification-rules/113826?camid=4v1a](www.igi-global.com/article/evolutionary-approaches-for-the-extraction-of-classification-rules/113826?camid=4v1a)

Fuzzy Cluster Analysis of Larger Data Sets
[www.igi-global.com/chapter/fuzzy-cluster-analysis-larger-data/38574?camid=4v1a](www.igi-global.com/chapter/fuzzy-cluster-analysis-larger-data/38574?camid=4v1a)