Abstract

Random Number Generator is an electronic circuit or it can be software or can be optimized architecture. In many practical applications such as cryptography, model simulation, sampling, games of chance, numerical analysis, there is a need of the generation of series of random number. This is achieved for ex. by means of tables, specific algorithms or electronic circuits. This Random number can be generated by either specific software or a FPGA based architectures. Field Programmable Gate Array (FPGA) optimized random number generator
Pseudo-Random Number Generation by Fibonacci and Galois LFSR Implemented on FPGA

(RNG) are more resource efficient than software optimized RNG because they can take the advantage of bitwise operations and FPGA specific features. Hence for generation of random number, FPGA architecture is generally used. By using different FPGA platform, random number can be generated. There are several algorithms by which the random number has been generated. Each algorithm had used a different FPGA platform for generation of random number. In this paper generation of 8 bit random number by means of two method i. e Fibonacci series method and Galois liner feedback shift register method. Moreover for analysis Altera platform is used i. e. for simulation Modelsim software and for synthesis Quartus II software is used. Hence by using these two algorithms, random numbers have been generated and each algorithm has shown different performance parameters i. e. area, speed and power.

References

- Ravi saini, Sanjay Singh, Anil Saini, AS Mandal, Chandra Shekhar CSIR- central electronics engineering research institutes (CSIR-CEERI) Pilani-Rajasthan, India 2013 on Design of a Fast and Efficient Hardware Implementation of a Random Number Generator in FPGA
- carols Gayoso, C. Gonzalez in 2013 on Pseudorandom Number Generator Based on the Residue Number System and Its FPGA Implementation in international conference on advance electronic system (ICAES)
- Yuan li, Paul Chow, Senior member IEEE, Jiang, Minxuan zhang, and shaojun wei in 2013 on Software / Hardware Parallel Long Period Random Number Generation Framework Based On The Well Method in IEEE Transactions
- David b. Thomas, member of IEEE and Wayne luk, fellow in April 2013 on A LUT-SR Family of Uniform Random Number Generators for FPGA Architecture IEEE transactions on very large scale integration system, Vol 21 no 4
- Jonathan M. Comer, Juan C. Cerda, Chris D. Martinez, and David H. K. Hoe in 2012 on Random Number Generators Using Cellular Automata Implemented on FPGA
- Ray C. C. Cheung, Student Member, IEEE, Dong-U Lee, Member, IEEE, Wayne Luk, Senior Member, IEEE ,in 2007 on Hardware Generation of Arbitrary Random Number Distributions from Uniform Distributions Via the Inversion Method
- jiang hanging, shaojun wei international conference on computer and information technology in 2012 on An efficient hardware random number generator based on MT method
- N. szaboo and R Tanaka in 1967 on Residue arithmetic and its application to computer technology M. soderstand, w Jenkins, jullien and F. Taylor in 1986 , residue number system arithmetic modern application in digital signal processing
- Savir., a new empirical test for quality of random integer generators
- Residue arithmetic a tutorial with examples. Computer magazines IEEE vol 1
- C. M. Gonzalez, H. A. larrondo xi workshop Implementations de sistemas caoticos en dispostivos logicos programmable
- Intensive stastical complexity measures of pseudorandom bit&amp;quot; by C. M. Gonzalez, H. A. larrondo
- A. Ross, H. larrondo, M mertin Generalized stastical complexity measures a new tool for dynamic systems

2 / 3
Pseudo-Random Number Generation by Fibonacci and Galois LFSR Implemented on FPGA

- Altera corporation www. altera. com FLEX 10K embedded programmable logic device family data sheet 2001
- F. Panneton, M. Mastumoto Improved long period generators based on the linear recurrences modulo 2 overview and comparison.
- Yuan li, Paul Chow, Senior member IEEE, Jiang, Minxuan zhang, and shaojun wei in 2013 on Hardware Parallel Long Period Random Number Generation Framework Based On The Well Method; IEEE Transactions On Very High Speed Large Scale Integration.

Index Terms

Computer Science

Circuit And Systems

Keywords

Random Number Generator Rng  Field Programmable Gate Array Fpga  Linear Feedback Shift Register Lfsr.