A BBS Random Number Generator for Low Power Applications

Volume 131

Number 3

Year of Publication: 2015

Authors:

Alireza Hassanzadeh, Vahid Mahboubi

10.5120/ijca2015907230

Abstract

In this paper a low power random number generator has been designed and implemented using BBS algorithm. The BBS random number generator is known for high statistical quality and power consumption. Dynamic power dissipation has been reduced significantly comparing to regular implementation. Low power techniques such as power gating and pipelining have been employed to reduce power consumption of the module. Experimental measurements for a 32-bit BBS random number generator shows at least 30% reduction in dynamic power consumption. The proposed low power BBS random number generator has been implemented on Xilinx Spartan-6 FPGA evaluation board.

References


Index Terms

Computer Science                        Power Systems

Keywords

RNG, BBS, Low power, VHDL, FPGA.