Hardware Gaussian Noise Generator

July 25 2016

Features

- Designed for hardware-based simulation system using Verilog.
- Based on the Box-Muller algorithm. Two 16-bit noise samples are generated every clock cycle.
- An implementation on a Xilinx Virtex-4 XC4VLX100-12 FPGA occupies 1452 slices, 3 block RAMs and 12 DSP slices, and is capable of generating 750 million samples per second at a clock speed of 375 MHz.
- The performance can be improved by exploiting concurrent execution: 37 parallel instances of the noise generator at 95 MHz on a Xilinx Virtex-II Pro XC2VP100- 7 FPGA generate seven billion samples per second, and can run over 200 times faster than the output produced by software running on an Intel Pentium-4 3 GHz PC.

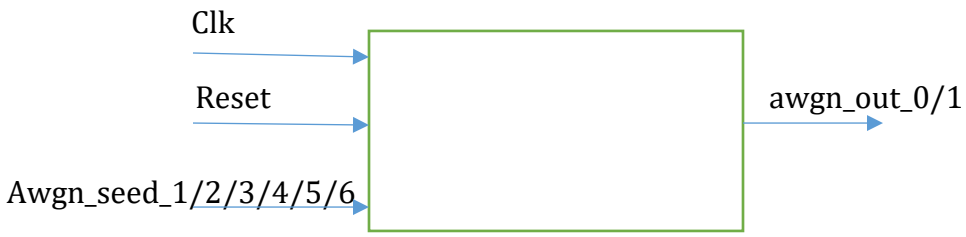
Product Specification

Design File Formats	Verilog
Verification	MATLAB + ModelSim + System Verilog
Simulation	ModelSim PE 10.4e

Applications

The noise generator is currently being used at the Jet Propulsion Laboratory, NASA to evaluate the performance of low-density parity-check codes for deep-space communications.

Core Schematic Symbol



Clk	Input	Clock that triggers all sequential elements on its rising edge
Reset	Input	Active high synchronous reset
Awgn_seed_1/2/--/6	Input	Is the 32 bit input seed to generate random number
Awgn_out_0/1	Output	Is the 16 bit output of noise generator

Functional Description

The Box-Muller method starts with two independent uniform random variables u0 and u1 over the interval [0, 1). The following mathematical operations are performed to generate two samples x0 and x1 of a Gaussian distribution N (0, 1).

- $e = -2\ln(u0)$
- $f = \sqrt{e}$
- $g0 = \sin(2\pi u1)$
- $g1 = \cos(2\pi u1)$

- x0 = f ×g0
- x1 = f ×g1

Traditional linear feedback shift registers (LFSRs) are often sufficient as a uniform random number generator (URNG), Tausworthe URNGs are fast and occupy less area. Furthermore, they provide superior randomness when evaluated using the Diehard random number test suite. Our Tausworthe URNG follows the algorithm presented by L'Ecuyer, which combines three LFSR-based URNGs to obtain improved statistical properties. It generates a 32-bit uniform random number per clock and has a large period of 2^88(≈ 10^25).

Design Verification

The design was tested using a System Verilog test bench which compares the output of design in Verilog with the output of golden model in MATLAB.

References

1. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1628955
2. M.J. Schulte and E.E. Swartzlander Jr., "Hardware designs for exactly rounded elementary functions," IEEE Trans. Computers, vol. 43, no. 8, pp. 964–973, 1994.
3. J. H. Mathews, Numerical Methods for Computer Science, Engineering and Mathematics. Englewood Cliffs, NJ: Prentice-Hall, 1987.