Abstract

In electronics communication systems random number generation is used for security purposes. The numbers which are in random but in predefined sequence pattern is called as pseudo random while the numbers which are unpredictable and in undefined sequence pattern is called as true random numbers. These random numbers are also used for bit error rate testing (BERT). When multiple bits are required then linear feedback shift registers are the best source of random number generator. The increase in length of random number sequence consumes more area. Here a increase length of sequence and multiple bits random number generator is designed using linear feedback shift registers and multiple port SRAM memory. The SRAM base random number generator is area efficient using VHDL. The improved computational time and throughput is computed using VHDL implementation.

References

1. Yuan Li, Paul Chow, Jiang Jiang, Minxuan Zhang, and Shaojun Wei "Software/Hardware
Parallel Long-Period Random Number Generation Framework Based on the WELL Method" Ieee Transactions On Very Large Scale Integration (Vlsi) Systems year 2013.


Index Terms

Computer Science
Circuits and Systems

Keywords

RNG, BERT, LFSR, SRAM