In electronics communication systems random number generation is used for security purposes. The numbers which are random but in a predefined sequence pattern are called pseudo-random numbers while the numbers which are unpredictable and in an undefined sequence pattern are called 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, an increase in 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


Index Terms

Computer Science
Circuits and Systems

Keywords

RNG, BERT, LFSR, SRAM