Gerador de Números aleatórios utilizando portas lógicas em PLDs

Otávio Terra Roque

Orientador: Maximiliam Luppe

Escola de Engenharia de São Carlos/ USP

otaviotroque@usp.br

Objetivos

Os dispositivos reconfiguráveis vem ganhando cada vez mais destaque em nossa sociedade atual, desta forma, aplicações utilizando esse tipo de tecnologia vem sendo cada vez mais recorrentes.

Outra necessidade que nosso mundo atual apresenta é a de conseguirmos maneiras de gerar números que são verdadeiramente aleatórios, tarefa essa que computadores podem apresentar certa dificuldade, vez que são máquinas altamente determinísticas.

Dessa forma unindo essa tecnologia ascendente dos dispositivos reconfiguráveis com a necessidade de um gerador de números aleatórios, temos como o objetivo desse trabalho o desenvolvimento desse tipo de gerador em um desses dispositivos.

Métodos e Procedimentos

Para o desenvolvimento dessa aplicação foi estudada uma topologia que já apresentou resultados positivos para essa aplicação mas que não foi implementada em uma FPGA como é proposto por esse trabalho.
Essa topologia é baseada em um oscilador caótico booleano que gerará os bits aleatórios que queremos obter como resultado final essa topologia é apresentada na figura a seguir.

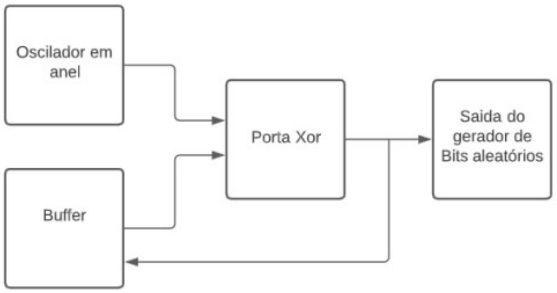

Figura 1: Topologia utilizada. Fonte: Autor

Seguindo o trabalho True random number generation using CMOS Boolean chaotic oscillator[1], onde é apresentado pelos autores um circuito oscilador caótico que foi usado como base para esse trabalho. Esse circuito é composto por portas lógicas do tipo NOT e uma porta lógica do tipo XOR e tem a configuração apresentada na figura a seguir.

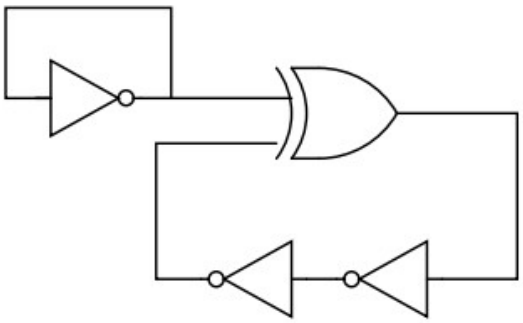

Figura 2: Gerador caótico booleano.
Fonte: True random number generation using CMOS Boolean chaotic oscillator. [1]

Com o estudo então desse tipo de configuração e do trabalho desenvolvido por RAJAGOPALAN S. RETHINAM, A. N. D. A. P. M. J. A. R. S.[2], onde é apresentada uma implementação de um gerador de bits aleatórios que se baseia no trabalho de PARK J. C. RODGERS, D. P. L. M.[1], foi implementado o seguinte circuito.

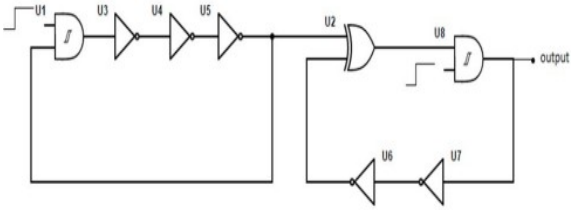

Figura 3: Circuito do gerador de bits aleatórios
Fonte: Design of Boolean Chaotic Oscillator using CMOS Technology for True Random Number Generation[2]

Esse então foi o circuito que foi implementado na FPGA durante o desenvolvimento desse trabalho.

Assim que obtivemos os bits gerados na FPGA foi submetido esses valores gerados a testes que mediram o grau de aleatoriedade do gerador, esses testes são testes padronizados pelo NIST (National institute of standards and technology) que é propõe uma série de 14 testes[3] para podermos classificar uma fonte de números aleatórios como sendo aleatória ou não.

Resultados

Após a implementação final e fazer a obtenção dos dados, os resultados obtidos foram submetidos a uma variedade de testes estatísticos[3] e após a realização destes testes foi verificado que o gerador apresentou resultados extremamente satisfatórios, sendo “aprovado” em todos os testes em que foi submetido. Os resultados que foram obtidos dessa sequência de testes foram os seguintes.

Teste realizado	P-valor obtido
Teste de frequência do monobit	0,08423
Teste de frequência em bloco	0,15157
Teste de corrida	0,15936
Mais longa execução de uns em um bloco	0,85488
Teste de classificação de matriz binária	0,19213
Teste da transformada discreta de Fourier	0,79396
Teste de correspondência de modelo sem sobreposição	0,6831
Teste de correspondência de modelo com sobreposição	0,85877
Teste de complexidade linear	0,01783
Teste Serial	0,7467
Teste da entropia aproximada	0,01597
Teste das somas cumulativas(Para frente)	0,15003
Teste das somas cumulativas(Para trás)	0,15003
Teste de excursões aleatórias	0,60591

Tabela 1: Resultados dos testes. Fonte: Autor

Para avaliar se um teste foi ou não bem-sucedido é preciso que o p-valor obtido seja maior que 0.01, e como podemos observar na tabela esse requisito foi cumprido em todos os testes.

Dessa forma foi possível concluir que a topologia utilizada aplicada em uma FPGA funciona perfeitamente para os propósitos propostos.

Conclusões

Então podemos concluir que o gerador de números aleatórios implementado na FPGA apresentou os resultados esperados e com isso abrem-se diversas portas para as mais inúmeras possibilidades de aplicações dessa tecnologia em problemas reais onde números aleatórios são realmente necessários.

Referências Bibliográficas

[1]PARK J. C. RODGERS, D. P. L. M. True random number generation using CMOS Boolean chaotic oscillator. [S.l.]: Microelectronics Journal, v. 46, pp. 1364–1370, 2015

[2]RAJAGOPALAN S. RETHINAM, A. N. D. A. P. M. J. A. R. S. Design of Boolean Chaotic Oscillator using CMOS Technology for True Random Number Generation. [S.l.]: IEEE, 2017.

[3]RUKHIN J. SOTO, J. N. M. S. E. B. S. L. M. L. M. V. D. B. A. H. J. D. S. V. A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. [S.l.]: National Institute of Standards and Technology, 2010.