Uso de Plataformas Embarcadas na caracterização de um Gerador Físico de Números Aleatórios

Aparecida Falcão de Andrade, Jorge Fredericson de Macedo Costa da Silva, Fábio Alencar Mendonça

***Resumo*—A geração de números aleatórios é uma técnica que possui inúmeras aplicabilidades: simulações numéricas para eventos meteorológicos, jogos, protocolos de segurança e criptografia, etc. Pode ser implementada por meio físico ou lógico. Utilizando método físico, chegamos a fontes de entropia não determinísticas fundadas em efeitos físicos aleatórios ou quânticos. Este trabalho propõe a criação de um sistema embarcado capaz de realizar leituras de uma fonte de entropia, baseada no efeito avalanche de semicondutores, e verificar as amostras com base nos testes propostos pela entidade certificadora para checar a eficiência do sistema apresentado para aplicações em Sistemas de Comunicações.**

Palavras-Chave—Geração de Números Aleatórios; Sistemas de Comunicações; Circuitos e Dispositivos de Comunicações.

***Abstract*— The generation of random numbers is a technique that has numerous applicabilities: numerical simulations for meteorological events, games, security protocols and cryptography, etc. It can be implemented physically or logically. Using the physical method, we arrive at nondeterministic entropy sources based on random or quantum physical effects. This work proposes the creation of an embedded system capable of performing readings of an entropy source, based on the avalanche effect of semiconductors, and verifying the samples based on the tests proposed by the certifying entity to check the efficiency of the presented system for applications in Communications Systems.**

Keywords—Random Number Generation; Communications Sytem; Circuit and Devices of Communications.

I. INTRODUÇÃO

Diversos ramos das Ciências Exatas e Engenharias carecem de números aleatórios para o estudo e análise de fenômenos atrelados à natureza. Estes números são obtidos através de geradores de números aleatórios (RNGs – *Random Numbers Generators*), que fazem uso de processos físicos, tais como decaimento de uma substância química ou turbulência em discos rígidos. Para geração de tais sequências outra forma seria com inclusão de um hardware ao sistema ou através de algoritmos para geração de sequências pseudoaleatórios baseadas em uma semente. Na literatura, algoritmos assim são facilmente encontrados, são exemplos: geradores congruentes lineares, autômato celulares, geradores baseados em sistemas caóticos, etc. [3]

A escolha de um gerador deve satisfazer os requisitos da aplicação destinada, ou seja, com margem nula para escolhas arbitrárias. Uma forma de avaliar a qualidade de um gerador de números pseudoaleatórios é por meio da execução de testes estatísticos. Para alguns procedimentos, isso nem sempre indicará qual metodologia ideal. Em geradores para fins criptográficos, a avaliação por testes estatísticos não é adequada para assegurar a escolha de um bom gerador. Em esquemas de Criptografia, os geradores são elementos primordiais e, portanto, considerados primitivas criptográficas [3].

Este trabalho visa caracterizar um gerador físico de números aleatórios, como também a prova das sequências geradas em um pacote estatístico composto de 15 testes que foram desenvolvidos para testar a aleatoriedade das sequências binárias produzidas por hardware ou software fornecidos pelo *National Institute of Standards and Technology* (NIST) em duas plataformas computacionais embarcadas.

II. GERADOR DE NÚMEROS ALEATÓRIOS

Um número aleatório é um número gerado por um processo cujo resultado não pode ser previsível e que futuramente não possa ser representado de maneira confiável [4].

Segundo [5], uma sequência de números aleatórios é uma sequência de números independentes com uma distribuição específica e uma probabilidade especifica para assumir qualquer valor em um dado intervalo de valores. De acordo com [6], uma sequência que tem as mesmas propriedades estatísticas como bits aleatórios, é imprevisível e não pode ser reproduzida de forma confiável.

Assim, Geradores de Números Pseudoaleatórios são, na maioria dos casos, modelos matemáticos que produzem sequências determinísticas a partir de uma entrada inicial, chamada semente. Já, Geradores Físicos de Números aleatórios são aqueles que usam algum princípio físico como base para geração das sequências e, em alguns casos, podem ser considerados aleatórios.

III. METODOLOGIA

A fonte de Entropia não determinística usada neste trabalho é baseada no efeito avalanche extraída por meio da polarização reversa da junção "pn" de um transistor polarizado reversamente com coletor aberto. Com o sinal gerado, ele é amplificado também por um transistor igual aos geradores do sinal, pois, ele apresenta baixo ruído. A alimentação do sistema é contínua e com um máximo de 18V, a depender do transistor usado e após a etapa de amplificação o sinal é limitado por um Diodo Zener de 4,7 V, para não danificar os componentes digitais usados, uma vez que todos são TTL (operam de 0 até 5V). A saída do sinal analógico passa por um inversor tipo *Schmitt Trigger* para depois ser lida pelas plataformas

Aparecida Falcão de Andrade, Jorge Fredericson de Macedo Costa da Silva, Fábio Alencar Mendonça, Departamento de Telemática, Instituto Federal do Ceará (IFCE), Fortaleza-CE, Brasil, E-mails: {cidafalcao18, jorge.fredericson, fam.alencar}@gmail.com. Este trabalho foi parcialmente financiado pelo CNPq (488402/2013-1).

computacionais embarcas, *Arduino Uno* e *Arduino Due*. Na Figura 1, é mostrado o circuito gerador de sinal.

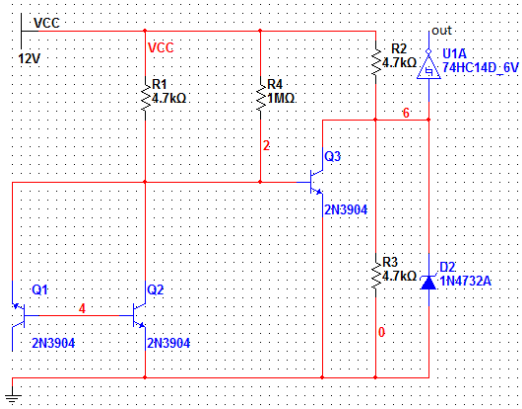

Fig. 1. Esquema elétrico do GFNA.

IV. Resultados e Discussões

A fonte de entropia baseada no efeito avalanche apresenta várias curvas a depender da tensão de alimentação do sistema que varia de um valor inicial a depender do transistor, devido ao seu processo de fabricação conter imperfeições e impurezas nos semicondutores, até o valor máximo de 18 volts. Então, temos duas curvas, uma com efeito avalanche na saída do transistor gerador e a curva após passar pelo ST já digitalizada. Elas podem ser observadas nas Figuras 2 e 3.

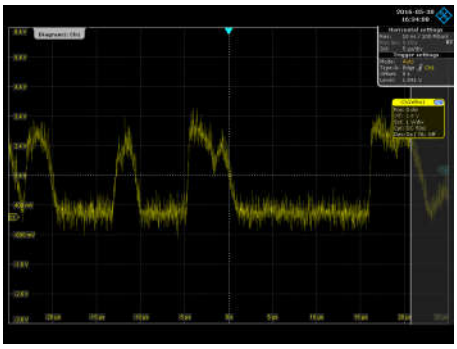

Fig. 2. Sinal analógico gerado pelo efeito avalanche.

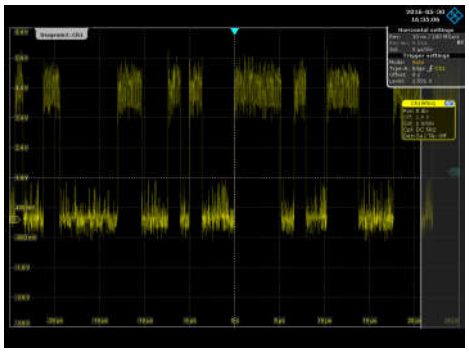

Fig. 3. Sinal digitalizado pelo *Schimitt Trigger*.

Os dados gerados são enviados para o Matlab© realizar o pós-processamento e execução de uma bateria de testes sugeridos pelo NIST, esta etapa é realizada por computador do tipo *Desktop*. O pós-processamento dos dados é feito baseado no algoritmo de von Neumann, Figura 4. Esse algoritmo é usado para manter a quantidade de zeros e uns tenderem a um equilíbrio.

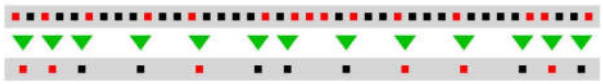

Fig. 4. Funcionamento do algoritmo de von Neumann.

Por meio desse algoritmo, grandes sequências de zeros e uns são evitadas a um custo computacional baixo. Por exemplo, os quadrados vermelhos podem ser os bits 1 e, portanto, os pretos serão os bits 0. Após o pós-processamento, há uma redução do número de bits, neste caso de 30 para 13, tal redução é chamada de eficiência do algoritmo.

TABELA 1.
Comparativo das Plataformas e seu desempenho nos Testes

Teste Estatístico	Arduíno UNO	Arduíno DUE
Frequência (Monobit)	SIM	SIM
Frequência de um Bloco	SIM	SIM
Teste de Corrida	NÃO	NÃO
Maior Corrida de uns dentro de um Bloco	NÃO	NÃO
Posto da Matriz Binária	SIM	SIM
Espectral da Transformada discreta de Fourier	SIM	NÃO
Casamento de padrão sem superposição	SIM	SIM
Casamento de padrão com superposição	SIM	SIM
Estatística universal de Maurer	SIM	SIM
Complexidade Linear	N/I*	N/I
Serial	NÃO	NÃO
Entropia Aproximada	NÃO	NÃO
Somas Cumulativas	N/I	N/I
Excursões Aleatórias	SIM	SIM
Variantes de excursão aleatória	SIM	SIM
*N/I – Teste não implementado		

V. Conclusões

Foi possível caracterizar uma fonte de entropia não determinística, baseada no efeito avalanche, em duas plataformas computacionais embarcadas. Os testes do NIST para esta fonte com alguns ajustes podem validar definitivamente o protótipo para sua fabricação e uso nas aplicações citadas. Ressalta-se o baixo custo da solução.

Agradecimentos

Ao apoio do PPGET/IFCE por meio do Laboratório GDESTE que permitiu a execução do projeto.

Referências

[1] J. E. Gentle, Simulating Random Numbers from a Uniform Distribution. Random number generation and Monte Carlo methods, p. 1–55, Maio 2003.

[2] E. J. L. Soares, Geradores quanto-ópticos de números aleatórios. 2013. Tese de Doutorado. Universidade Federal do Ceará.

[3] E. B. G. Costa, Ataques Quânticos a Geradores de Números Pseudo-Aleatórios. Centro de Engenharia Elétrica e Informática. 2011. Tese de Doutorado. Universidade Federal de Campina Grande.

[4] I. D. Quantique, White paper: Random number generation using quantum physics. ID Quantique SA, Switzerland, Tech. Rep. Version, v. 3, 2010.

[5] D. Knuth, The art of computer programming, 2nd Ed., Editora Adisson Wesley,1981,vol 2.

[6] B. Schneier, Applied Cryptography Second Edition: protocols, algorithms, and source code in CJ Wiley & Sons. 1996. NIST. Natl. Inst. Stand. Technol. Spec. Publ. 800-22rev1a, 131 pages

[7] (April 2010). Disponível em: <csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf>. Acesso em: 01 set. 2015.