UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
BACHAREL EM ENGENHARIA ELÉTRICA

Pedro Augusto Böckmann Alves

DESENVOLVIMENTO DE TRNG (TRUE RANDOM NUMBER GENERATOR) ATRAVÉS DE CÉLULAS MEMRISTORAS

Porto Alegre
2. Semestre
2022

Pedro Augusto Böckmann Alves

DESENVOLVIMENTO DE TRNG (TRUE RANDOM NUMBER GENERATOR) ATRAVÉS DE CÉLULAS MEMRISTORAS

Trabalho de Conclusão do Curso de Engenharia Elétrica da Escola de Engenharia da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do Título de Engenheiro Eletricista.

Orientador: Prof.ª Dr.ª Gilson Wirth

Porto Alegre
2. Semestre
2022

AGRADECIMENTOS

Agradeço ao professor Gilson Wirth, aos colegas bolsistas de iniciação científica e à UFRGS como um todo por todo o conhecimento e orientação fornecidos, sem os quais esse trabalho não teria sido possível.

RESUMO

A criptografia segue sendo um tópico cada vez mais predominante na literatura, com a sua importância crescente, devido, sobretudo, ao desenvolvimento de processadores cada vez mais rápidos e tecnologias cada vez mais interconectadas. Sendo assim, o seguinte trabalho se propõe a idealizar um dispositivo conhecido como TRNG (True Random Number Generator, ou, em português, Gerador de Números Aleatórios Verdadeiros). TRNG é um dispositivo que gera números aleatórios a partir de um processo físico, e não por meio de um algoritmo. Tais dispositivos são frequentemente baseados em fenômenos microscópicos que geram sinais de "ruído" estatisticamente aleatórios de baixo nível, como ruído térmico, efeito fotoelétrico, ou fenômenos quânticos. Esses processos estocásticos são, em teoria, completamente imprevisíveis enquanto uma equação que governa tais fenômenos for desconhecida ou incomputável. Isso contrasta com o paradigma de geração de números pseudo-aleatórios comumente implementado através de algoritmos. As sequências de números são usadas em diversos processos, dentre os quais a criptografia. O dispositivo desenvolvido terá a necessidade de ser compatível com a tecnologia atual, propondo-se a sanar a demanda criptográfica cada vez mais latente, dando confiabilidade e segurança aos sistemas computacionais. Utilizaremos no seguinte estudo o conceito de TRNG's baseados em RTN (Random Telegraph Noise), um ruído de características aleatórias, presente em semicondutores. O RTN será obtido de células conhecidas como memristoras. Embora a ideia de TRNG's baseados em RTN não seja nova na literatura, o estudo fará a análise em células com diferentes semicondutores, um dos quais, o hBN (nitreto de boro hexagonal), ainda pouco estudado.

Palavras-chave: Criptografia; RTN; TRNG, Memristores.

ABSTRACT

Cryptography continues getting more prominent in the literature, with its importance growing due to the development of faster computer processing and more interconnected technologies getting available (IoT). Therefore, the following study will develop a device known as TRNG (True Random Number Generator). TRNG is a device that generates random numbers from a physical process, not through an algorithm. Such devices are often based on microscopic phenomena that generate low-level, statistically random "noise" signals, such as thermal noise, the photoelectric effect, or quantum phenomena. These stochastic processes are, in theory, completely unpredictable as long as an equation governing such phenomena is unknown or uncomputable. This contrasts with the pseudo-random number generation paradigm commonly implemented through algorithms. The developed device needs to be compatible with today's technology, solving the present growth of cryptographic need, offering reliability and security to computational systems. We will use the concept of RTN (Random Telegraphic Noise) based TRNG's. RTN is a noise of random characteristics, present in semiconductors. This RTN will be obtained from cells known as memristors. Although the idea of RTN based TRNG's is not new, this study will analyze cells with a variety of semiconductors, one of which, hBN (hexagonal boron nitride), still not very studied.

Keywords: Cryptography; RTN; TRNG, memristors.

SUMÁRIO

1 INTRODUÇÃO

Com a diminuição das dimensões dos dispositivos, oriunda do desenvolvimento da microeletrônica, certos desafios e problemas de confiabilidade se tornam cada vez mais preponderantes. Como expoente dos presentes desafios da indústria, temos um ruído conhecido como RTN (Random Telegraph Noise). O RTN se caracteriza como uma variação abrupta dos níveis de corrente de dispositivos semicondutores, sendo originado pela captura e emissão de portadores de carga em defeitos presentes no material.

Apesar de ser caracterizado na maior parte das aplicações como um ruído, causando problemas para o uso em massa de memristores e originando o ruído de fase em sinais de telecomunicação, também há possíveis aplicações para esse fenômeno, tais como a geração de sinais verdadeiramente aleatórios e aplicações na criptografia, que será tema do seguinte estudo. As características aleatórias de uma armadilha de RTN o tornam um objeto de estudo interessante ao desenvolvimento de TRNG's (True Random Number Generator, ou, em português, Gerador de Números Aleatórios Verdadeiros). Além disso, o RTN é um efeito comum aos semicondutores de maneira geral, tornando a fabricação de uma célula de TRNG baseada em RTN compatível com a indústria atual, diminuindo-se assim, os seus custos de fabricação.

1.1 MOTIVAÇÃO

A criptografia, de uma forma geral, é um escopo que tem a sua relevância crescente, com o desenvolvimento de processadores cada vez mais poderosos, capazes de burlar algoritmos sofisticados, e uma necessidade cada vez maior de confiabilidade e segurança, com a emergência de conceitos como a internet das coisas (IoT), que expõem a emergência de um mundo cada vez mais interconectado.

Nesse contexto, o desenvolvimento de TRNG's é um desafio bastante atual, com uma diversidade de estudos e artigos sendo publicados sobre o tema, o que demonstra o potencial da área de estudo. Soluções incompatíveis com a tecnologia atual, dispositivos que não apresentam uma frequência de geração de números

aleatórios satisfatória e TRNG’s com uma vida útil pequena são problemas atuais que revelam a necessidade de uma solução inovadora.

1.2 DESCRIÇÃO DO PROBLEMA

O processo de desenvolvimento do TRNG se dará, primeiramente, através da validação de todo o processo de aquisição das medidas, isto é, a simulação do circuito de geração de número aleatório e a validação da aleatoriedade do seu resultado. Uma vez atestado que esse processo funciona, as medidas reais então serão analisadas e processadas e novamente será determinada a qualidade dos resultados obtidos, dessa vez de uma forma mais criteriosa. Os resultados obtidos então poderão ser comparados às soluções já presentes na literatura.

1.3 RELEVÂNCIA DA SOLUÇÃO

Uma abordagem diferenciada na produção de TRNG's, que apresente bons resultados, caracterizaria um avanço significativo dessa tecnologia, tornando seu uso e fabricação em massa mais próximos da realidade e, possivelmente, resolvendo alguns problemas existentes no atual uso do RTN para TRNG’s.

1.4 DELIMITAÇÃO DO ESCOPO

O presente estudo se proporá a usar medidas próprias de dispositivos memristores MIM (Metal-Isolante-Metal), obtidas no laboratório LCE (Laboratório de Caracterização Elétrica da UFRGS), e, para extração dos parâmetros dos RTN’s medidos, também serão usados algoritmos e códigos próprios. Será realizada, também, uma análise mais aprofundada dos resultados provenientes dos diferentes semicondutores, estabelecendo-se assim possíveis relações entre a qualidade dos números gerados e determinar possíveis especificidades e potencial das amostras analisadas.

1.5 DEFINIÇÃO DOS OBJETIVOS

As fases de leitura, processamento das medidas e construção de algoritmo para identificação de amostras são a definição do estudo que será desenvolvido. Após a execução dessas etapas, a avaliação e comparação da eficiência da solução desenvolvida com as tecnologias e algoritmos estado da arte também será estudada. É prevista a avaliação da resposta de cada um dos semicondutores estudados e também uma definição mais abrangente da qualidade do TRNG desenvolvido.

2 FUNDAMENTAÇÃO TEÓRICA

O estudo do ruído conhecido como RTN se tornou cada vez mais preponderante com o avanço da microeletrônica e escalonamento dos dispositivos semicondutores (WIRTH, 2020). Na literatura, há uma infinidade de novos artigos publicados sobre o tema, evidenciando o potencial de novas descobertas e estudos na área. O escopo que se dá a esse estudo é comumente o de minimização de tal ruído, bem como o entendimento dos processos envolvidos, buscando auxiliar projetistas de circuitos a projetar circuitos confiáveis e de alto desempenho, apesar do ruído onipresente. As variabilidades presentes nos dispositivos semicondutores são geralmente tidas como desafios para indústria, já que para a maior parte das aplicações é necessária a padronização dos dispositivos e, também, a previsibilidade na sua operação, duas características que vão de encontro aos efeitos provocados pelas armadilhas de RTN.

Considerando toda essa base científica de estudo do RTN como ruído, temos uma área muito menos explorada e desenvolvida. O RTN é uma característica intrínseca de cada dispositivo, tendo, assim, propriedades que são interessantes para usos específicos. Considerando todas as características do RTN apresentadas, existe algumas aplicações que ainda podem ser melhor exploradas. Uma dessas aplicações é a de RNG (Random Number Generator).

A geração de números aleatórios (RNG) é um escopo que encontra uma vasta gama de aplicações, que inclui simulações, estatística e, com a importância cada vez maior, a criptografia.

2.1 FUNDAMENTAÇÃO E CARACTERIZAÇÃO DO RTN NA LITERATURA

Sendo o RTN o princípio de funcionamento do dispositivo que o nosso estudo se propõe a desenvolver, faz-se necessário embasamento do estado da arte de entendimento de tal ruído, fundamentando-se suas propriedades e características.

De um ponto de vista teórico-físico, o RTN é a captura ou emissão de portadores de carga devido à presença de uma falha em um semicondutor. Esse fenômeno só é significativo por conta do dimensionamento dos dispositivos e das grandezas elétricas cada vez menores. O ruído é caracterizado como sendo estocástico, isto é, verdadeiramente aleatório, com o próximo estado de condutância independente do anterior. As armadilhas de RTN, por sua vez, se caracterizam por sua amplitude, tendo seus tempos de captura e emissão uma distribuição exponencial (NAGUMO *et al.*, 2010).

De uma forma sucinta, o RTN pode ser descrito como transições abruptas e discretas de uma grandeza elétrica em análise, em que, no contexto de um dispositivo MOSFET, por exemplo, pode ser observada na corrente de dreno e também a tensão de threshold Vt. Analisando o domínio frequência, também temos o padrão de densidade espectral de cada armadilha, que descreve uma distribuição de Lorentz (WIRTH; DA SILVA; BOTH, 2021).

(WIRTH; DA SILVA; BOTH, 2021), modela o RTN de uma forma estatística, fazendo algumas considerações que são interessantes para o nosso estudo, como caracterizá-lo como um efeito estocástico, isto é, aleatório, sendo a sua constante de tempo uma variável aleatória distribuída de uma forma logarítmica. Também, segundo o autor, uma possível modelagem para o RTN tem a característica de ter o número de armadilhas como uma variável aleatória, que segue a distribuição de Poisson.

Em uma medição de RTN é possível que o sinal seja complexo e não haja apenas uma única armadilha em ação. Para a construção de nosso TRNG, é também necessária uma discussão a respeito da caracterização de múltiplas armadilhas na mesma amostra. Comumente na literatura é aceita a hipótese de que as diferentes armadilhas presentes num dispositivo poderão ser analisadas de uma forma independente, ou seja, as suas amplitudes simplesmente se somarão, sendo os níveis

presentes numa amostra a soma dos níveis de corrente de cada armadilha. Entretanto, sob uma perspectiva mais verosímil, há efeitos ditos de acoplamento entre as diferentes armadilhas. Há modelos, por exemplo, de acoplamento elétrico das amplitudes das armadilhas dos dispositivos, de forma que a grandeza resultante não é simplesmente a superposição dos estados de cada armadilha (BECKER *et al.*, 2020). Para um estudo completo acerca da construção de um TRNG viável é necessário também uma discussão e ponderação a respeito.

Também é importante salientar as dificuldades existentes para a correta medição e detecção do RTN, que podem impactar a construção do TRNG. Temos como exemplo a necessidade de múltiplas medições para a caracterização correta de uma armadilha, constantes de tempo muito lentas, de forma que o processo de medição se torne demasiadamente longo (períodos de até 1 hora, por exemplo (ABE *et al.*, 2009)), armadilhas rápidas demais, o que torna a resolução de muitas topologias de detecção de RTN demasiadamente pequena e formas de onda complexas, considerando todos os efeitos de acoplamento no sinal (NAGUMO *et al.*, 2009) e possíveis ruídos que interfiram na medição, dificultando, assim, o processamento das medidas.

2.2 ESTADO DA ARTE NO DESENVOLVIMENTO DE TRNG's:

A primeira diferenciação básica que podemos fazer entre os diferentes geradores de números aleatórios é sobre sua implementação. Os geradores podem ser caracterizados por serem baseados em efeitos físicos, ditos como geradores baseados em hardware, ou true random number generators (TRNG) e os geradores baseados em algoritmos, ou pseudo random number generators (PRNG). Os TRNG são verdadeiramente aleatórios desde sua origem, baseados em fenômenos físicos estocásticos, enquanto os PRNG baseiam sua implementação num evento não estocástico, mas através de algoritmos computacionais o processam, de modo que, para uma gama específica de aplicações, o número gerado se comporte como um número verdadeiramente aleatório. Um exemplo de algoritmo PRNG estado da arte vastamente utilizado é Mersenne Twister (ROHE; ADVISOR; ALKASSAR, 2003)

Quanto ao desenvolvimento de geradores de números aleatórios baseados em hardware, ou TRNG, pode-se citar exemplos clássicos e comumente empregados, como o jogo de dados, cara ou coroa , roleta, etc. Em aplicações mais complexas, que requeiram, por exemplo, uma taxa de amostragem mais alta e integração com sistemas eletrônicos, temos tecnologias mais complexas, como as baseadas em decaimento radioativo (ROHE; ADVISOR; ALKASSAR, 2003), caos óptico (CHAMPAGNE; BISHOP, 2003), transições entre estados quânticos (HERRERO-COLLANTES; GARCIA-ESCARTIN, 2017) e o nosso escopo de estudo, o RTN (BROWN *et al.*, 2018).

1.

2.3 ESTADO DA ARTE DO USO DE RTN PARA DESENVOLVIMENTO DE TRNG's:

A discussão do RTN como princípio por trás do desenvolvimento de TRNG é um campo de estudo novo e fértil na literatura, com alguns empecilhos para o seu avanço. A manutenção do caráter verdadeiramente aleatório dos números gerados, validado através de testes de aleatoriedade, juntamente com a operação numa frequência alta são os problemas mais comumente encontrados (BREDERLOW *et al.*, 2006). Diferentes abordagens apresentam diversos graus de sucesso tentando sanar as limitações dessa implementação, tendo a tecnologia atual chegado a uma frequência de 5 Mbps de geração de números aleatórios (BROWN *et al.*, 2018).

Tendo em vista o que já foi desenvolvido até então, concluímos que a elaboração de uma abordagem inédita para o uso do RTN como mecanismo para construção de um TRNG encontra um espaço muito fértil na literatura. O resultado da pesquisa desenvolvida poderá ser comparado de uma forma satisfatória com a literatura já existente e a conclusão do trabalho trará uma perspectiva interessante do que foi desenvolvido frente ao que já existe.

3 METODOLOGIA

O desenvolvimento de nosso protótipo de gerador de números aleatórios passa pelas etapas de prova de conceito e de validação da nossa base de dados. A

prova de conceito refere-se à simulação de todo processo que será executado pelo nosso circuito eletrônico a ser desenvolvido. Já a validação de nossa base de dados é a verificação de que os dados provenientes das medidas do laboratório realmente servem a nosso propósito, isto é, são aleatórias.

2.

3.1 CONJUNTO DE TESTES NIST PARA VALIDAÇÃO DE ALEATORIEDADE

A validação requer um tipo de teste, que mostre que os dados, provenientes de cada uma das etapas desenvolvidas, são realmente aleatórios. Sendo assim, há a necessidade de uma norma ou padrão que seja usado como referência para a validação do nosso resultado.

O NIST (National Institute of Standards and Technology) (SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, 2019) é uma agência governamental estadunidense responsável por desenvolvimento de tecnologia, convenções e padrões regulatórios. Dentro das atribuições do NIST, há a elaboração de um conjunto de normas e recomendações para segurança criptográfica, o qual incorpora um protocolo para a validação de uma sequência de números como aleatória. Esse protocolo, chamado de Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (Conjunto de Testes estatísticos para Geradores de Números Aleatórios e Pseudoaleatórios para Uso em Aplicações Criptográficas) (BASSHAM *et al.*, 2010) será aqui empregado para validação de nosso gerador.

De uma maneira um pouco mais específica, o protocolo NIST assume que sequências aleatórias apresentam algumas características comuns, como, por exemplo, a uniformidade, escalabilidade e consistência. Esses termos, de acordo com os testes implementados, têm o seguinte significado:

- Uniformidade: Uma sequência aleatória com uma quantidade de bits significativamente longa, apresentará, aproximadamente, a mesma quantidade de 0’s e 1’s. Isso se deve ao fato de que, em um número binário aleatório, há a mesma probabilidade de haver, por caractere, um 0 ou um 1.

- Escalabilidade: Se uma sequência inteira é aleatória, subsequências também o serão. Isto significa que se dividirmos uma sequência inteira em subconjuntos, no caso de um número aleatório, esses subconjuntos também serão aleatórios. Dentro do protocolo, isso significa que esses subconjuntos também passarão por testes de aleatoriedade.

- Consistência: O número mantém sua aleatoriedade partindo de múltiplas ocorrências de fenômenos físicos. No estudo aqui desenvolvido, por exemplo, essa característica significa que o gerador produzirá as sequências de números usando como base diferentes transições de RTN e as características aleatórias serão mantidas, caso sua aleatoriedade seja atestada.

Partindo dessas características, que são usadas pelo NIST como a definição de um número aleatório, são então determinadas ferramentas estatísticas para a verificação da presença destas em um determinado número. Essas ferramentas, que em última instância definem o próprio protocolo, são um conjunto de quinze testes, que, de uma maneira bastante simplificada, tem a seguinte composição e definição:

1. The Frequency (Monobit) Test -Teste de Frequência (Monobit): O foco desse teste é determinar a frequência de 0's e 1's na sequência numérica. Esse teste verifica a característica de uniformidade no número analisado.

2. Frequency Test within a Block – Teste de Frequência dentro de Subconjuntos: Esse teste repete o teste número 1, mas dentro de subconjuntos do número original, validando-se assim os princípios de uniformidade e escalabilidade.

3. Runs Test – Teste de Transições: Esse teste valida as sequências de 0's e 1's, determinando o comprimento de sequências de bits repetidos,

verificando se a velocidade de transição dessas sequências é condizente com um número aleatório.

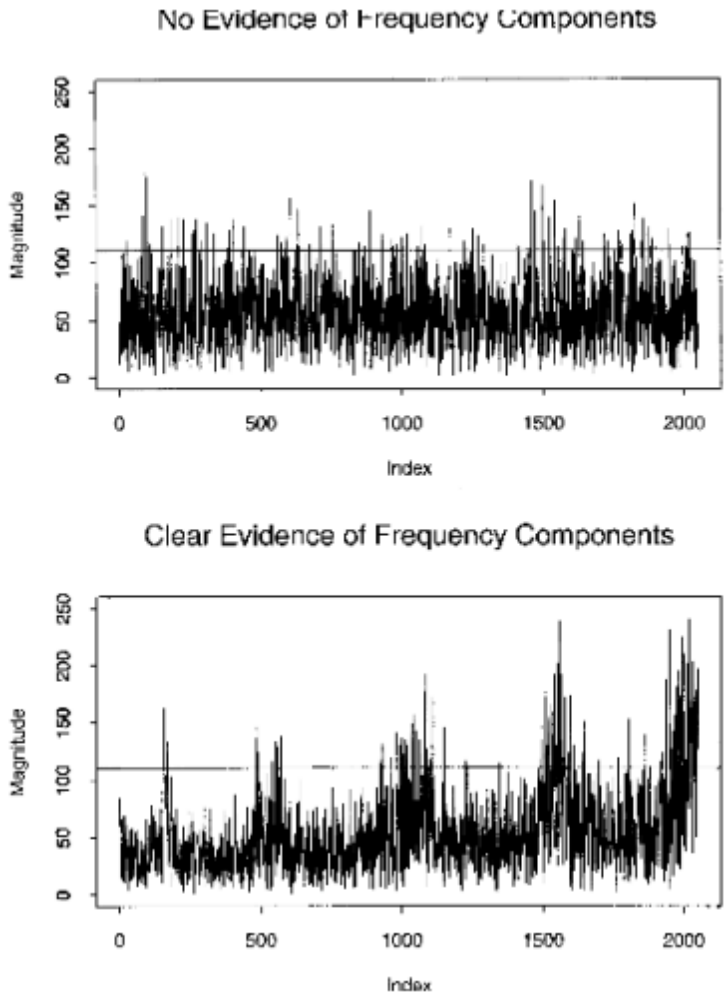
4. Test for the Longest Run of Ones in a Block – Teste de Número Máximo de 1’s em Sequência em um Subconjunto: Esse teste incorpora o princípio da uniformidade, analisando as sequências de 1’s repetidas. Não é necessário repetir o teste para sequências de 0, já que o resultado desse teste será o mesmo.

5. Binary Matrix Rank Test – Teste do Posto de Matrizes Binária: Esse teste faz uso do conceito de álgebra linear de posto matricial, que, por definição, é o conjunto de linhas ou colunas linearmente independentes de uma matriz. A implementação que se dá no teste é a divisão do conjunto de bits em matrizes quadradas, arbitrariamente de 32 linhas, em que cada bit ocupa uma posição da matriz, e o restante dos bits que não têm número suficiente para compor uma matriz são descartados. Depois disso, analisa-se o conjunto das matrizes, determinando seus postos e, finalmente, determinando a quantidade de matrizes em cada um dos 32 possíveis postos. Após isso, através de uma função, o teste determina a aleatoriedade ou não da amostra. Cabe salientar que uma maior quantidade de matrizes com postos de mais alto valor tende a validar a aleatoriedade.

6. Discrete Fourier Transform (Spectral) Test – Teste da Transformada Discreta de Fourier (Espectral): Esse teste consiste em converter a ocorrência de 0’s e 1’s ao domínio frequência, através da transformada discreta de Fourier, e identificar uma prevalência significativa de periodicidade na amostra. A determinação de uma periodicidade que reprova o caráter aleatório do número analisado é feita através da análise dos componentes no domínio frequência em que, se mais de 5% dos valores do domínio frequência passarem de certo limite calculado, o teste classifica a amostra como não aleatória. A Figura 1

mostra, na parte de cima e na parte de baixo, números no domínio frequência sem e com periodicidade, respectivamente.

Figura 1 – Amostras de Sequência de Números no Domínio Frequência



Fonte: BASSHAM *et al.* (2010, p. 70)

7. Non-Overlapping Template Matching Test – Teste de Ocorrência de Sequência Não Sobreposta: Esse teste rejeita números que apresentem uma ocorrência muito alta ou muito baixa para uma sequência dada como parâmetro, previamente definida. Cabe salientar que essa sequência que é fornecida para teste precisa ser aperiódica.

8. Overlapping Template Matching Test - Teste de Ocorrência de Sequência Sobreposta: Esse teste rejeita números que apresentem uma ocorrência muito alta ou baixa para uma sequência de bits 1.

Embora comumente usada com uma sequência de bits igual a 1, esse teste pode ser executado com qualquer ocorrência periódica arbitrária.

9. Maurer's "Universal Statistical" Test – Teste de Maurer Universal de Estatística: Introduzido inicialmente em 1992 por Ueli Maurer do departamento de Ciência da Computação da Universidade de Princeton, esse teste pode ser sumarizado com base na ideia de que um número aleatório não pode ser comprimido significativamente. Esse teste requer uma quantidade significativa de bits, necessitando de, no mínimo, 387840 bits.

10. Linear Complexity Test – Teste de Complexidade Linear: Esse teste é baseado no conceito de LFSR, Linear Feedback Shift Registers. A complexidade linear é, então, o polinômio de conexão LFSR de menor tamanho capaz de gerar os primeiros n termos da sequência. Existe, então, um algoritmo baseado nessa grandeza de complexidade linear para determinar a natureza aleatória do número gerado.

11. Serial Test – Teste Serial: O teste serial generalizado tem a ideia de testar a uniformidade da distribuição de subconjuntos de determinado tamanho na sequência numérica original.

12. Approximate Entropy Test – Teste de entropia aproximada: O conceito de entropia está ligado a desordem da amostra. Sendo assim, esse teste examina a regularidade de subconjuntos da sequência numérica

13. Cumulative Sums (Cusum) Test – Teste de Somas Cumulativas: Esse teste se baseia na atribuição de valores de +1 aos bits 1 e -1 aos bits 0, de modo que seja possível atribuir uma soma a subconjuntos da sequência numérica. Sendo assim, valores para as somas parciais altos indicam predominância de bits 1 e valores iguais a 0 significam

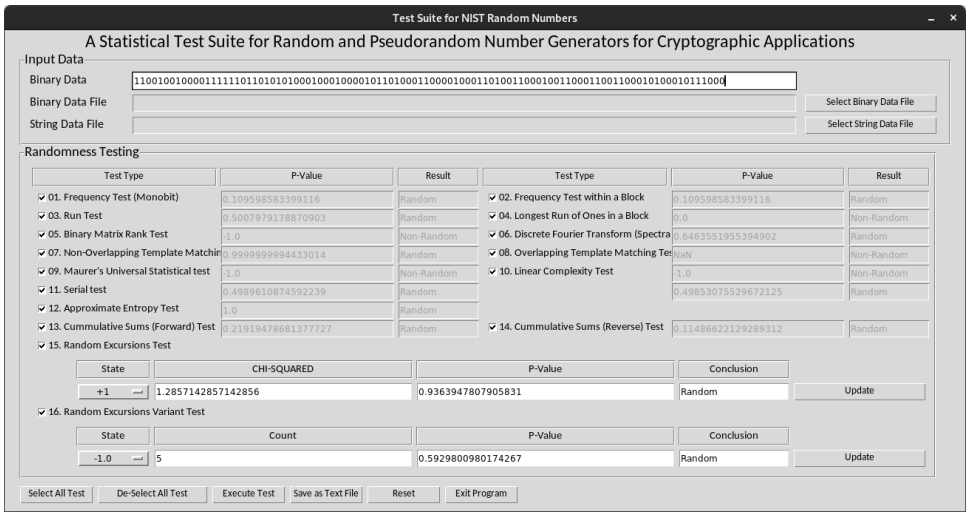
uma distribuição mais uniforme. Utilizando esses conceitos, é então feita uma análise dos máximos absolutos dessas somas parciais.

14. Random Excursions Test – Teste de Excursões Aleatórias: Utilizando a mesma ideia do teste 13, atribuindo-se valores de 1 e -1 aos bits 1 e 0 respectivamente, esse teste baseia-se na ideia de soma sucessiva da sequência numérica, índice a índice, com cada excursão sendo definida pelo início e volta em 0 da soma parcial. A avaliação de aleatoriedade se dá pela análise da tendência de estabilização da soma parcial em valores inteiros específicos ou, também, pela ausência de um número suficientemente grande de excursões.

15. Random Excursions Variant Test – Teste Variante de Excursões Aleatórias: Versão modificada do teste 14, em que a aleatoriedade da sequência numérica será determinada pela distribuição do número de visitas a um valor x de um determinado número de excursões (no mínimo quinhentas).

Dessa forma, foi contextualizado de uma forma um pouco mais aprofundada os testes de aleatoriedade do protocolo NIST. Resta definir a implementação desses testes. A versão do testador NIST que foi implementada no estudo foi um algoritmo de Python que incorpora cada um dos testes descritos, de autoria de (KHO ANG; CHURCHILL, 2022).

Figura 2 - Janela principal do Testador que implementa o NIST



Fonte: Imagem de Elaboração Própria, software de autoria de (KHO ANG; CHURCHILL, 2022) .

A Figura 2 demonstra a interface da implementação do protocolo NIST. Além dessa implementação do NIST para a testagem dos resultados de cada etapa, é necessária uma base de dados para referência. Um gerador de números aleatórios baseado em flutuações quânticas foi o escolhido, tendo como princípio de funcionamento a medição de campo magnético no vácuo (ANU QRNG, 2022).

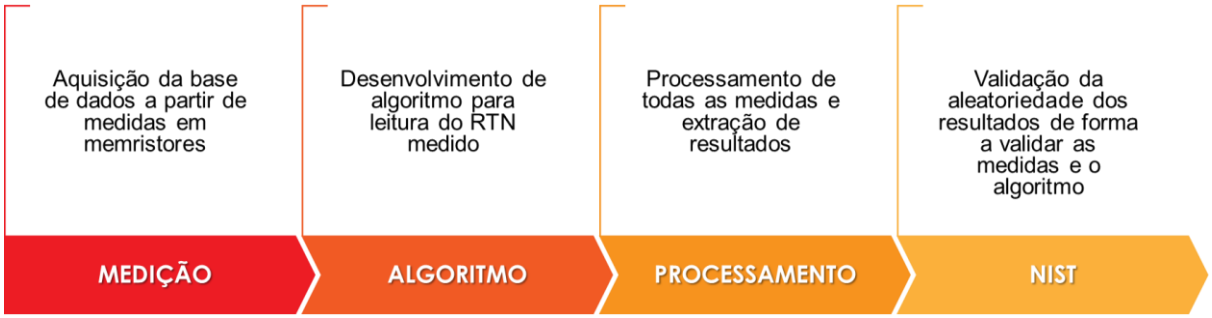
3.2 ETAPAS GERAIS PARA REALIZAÇÃO DO ESTUDO

De uma forma mais específica, a solução do trabalho proposto será implementada através das seguintes etapas: Criação e validação de RTN sintético através de base de dados verdadeiramente aleatória, captura de tempos de captura desse RTN sintético, uso dos tempos de captura para alimentação de contador de 8 bits, simulado via Spice, teste e validação da saída da simulação, elaboração de algoritmo para leitura dos tempos da base de dados oriunda de amostras reais e validação da aleatoriedade dos tempos de captura dessas amostras. A seguir, nas figuras 3 e 4, são demonstradas as etapas do trabalho.

Figura 3 - Etapas de Validação do Sistema de Aquisição de Medidas

Fonte: De autoria própria.

Figura 4 - Etapas da Validação da Base de Dados Obtida no LCE



Fonte: De autoria própria.

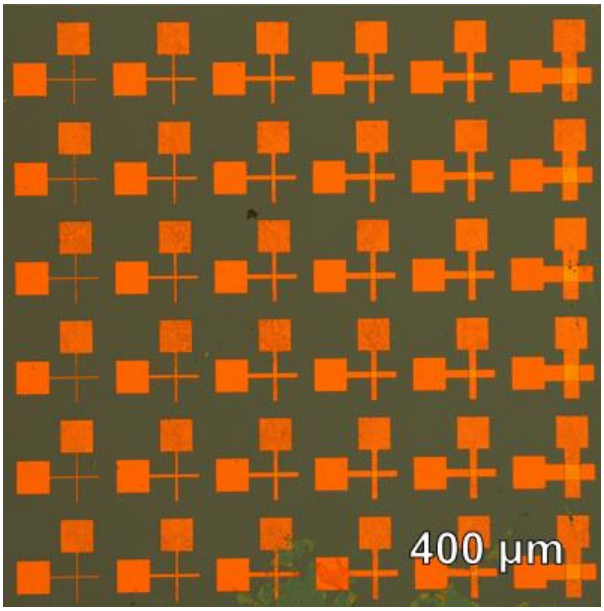
3.3 AQUISIÇÃO DA BASE DE DADOS

A validação da base de dados é parte fundamental da solução. Sendo assim, o primeiro passo é a medição em dispositivos memristores, afim de adquirir a maior quantidade possível de medidas que contenham RTN.

3.3.1 Amostras Utilizadas:

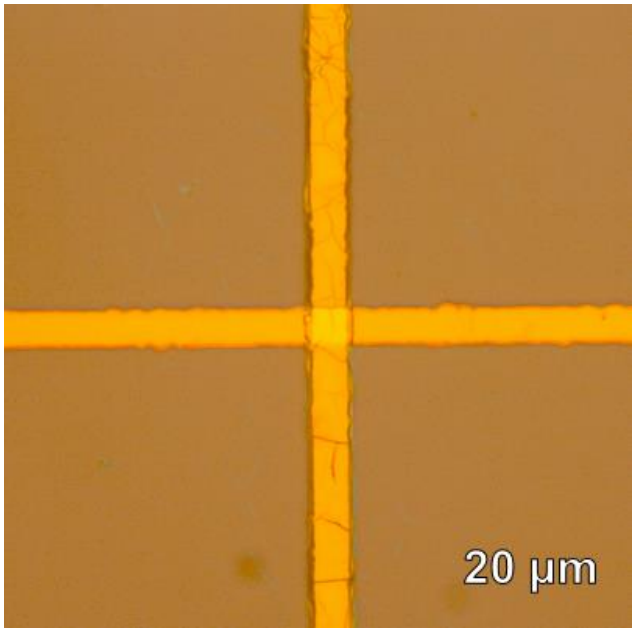
A medição foi realizada em células de três diferentes materiais semicondutores, o nitreto de boro hexagonal (hBN), o óxido de háfnio (HfO) e o dióxido de titânio (TiO2).

Figura 5 - Células memoristoras de hBN utilizadas



Fonte: Li, Xuehua (2020).

Figura 6 - Ampliação da Figura 5



Fonte: Li, Xuehua (2020).

Nas Figuras 5 e 6, é mostrado com mais clareza uma célula memristora de hBN. Os retângulos presentes na Figura 5 são os contatos das ponteiras. Já na Figura 7, temos em destaque a célula memristora em si, localizada na intersecção entre as

trilhas provenientes das duas ponteiras. Esse memoristor tem dimensão de 5 µm x 5 µm.

Figura 7 - Diferentes camadas da célula apresentada

Fonte: Li, Xuehua (2020).

3.3.2 Equipamentos Utilizados:

As medidas utilizadas foram obtidas no laboratório de caracterização elétrica da UFRGS (LCE). Os equipamentos usados no processo de experimentação foram o *4156C Precision Semiconductor Parameter Analyzer* (Figura 8) e, para as ponteiras, Cascade microtech EP6 (Figura 9). A resolução da medição para o analisador é de 1 fA para medidas de corrente, e de 0.2 µV para as medidas de tensão.

Figura 8 - 4156C Precision Semiconductor Parameter Analyzer

Fonte: Foto disponível em https://avalontest.com/keysightagilent-4156c-semiconductor-parameter-analyzer. Acesso em 17 set. 2022.

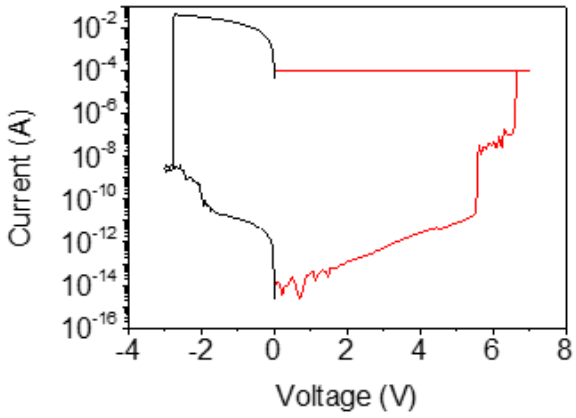
Figura 9 - Cascade microtech EP6

Fonte: Foto disponível em https://innoscope.ru/engineering/equipment/20863/. Acesso em 17 set. 2022.

3.3.3 Estado de Resistência das Células Memristoras:

Tratando-se de células memristoras, a base de dados incluí medições nos estados de alta resistência, baixa resistência e, em alguns casos, em estado indefinido (BECKER *et al.*, 2022). O estado de SET e RESET das células é também salvo no banco de dados.

Figura 10 - Processo de Set e Reset de uma célula de hBN



Fonte: Li, Xuehua (2020).

Na Figura 10 é mostrado o processo de Set e Reset de uma célula memristora. O estudo buscou englobar testes em ambos os estados e também determinar uma possível correlação entre um determinado estado e a frequência de bits aleatórios gerados (um indicativo da qualidade da solução proposta).

3.4 VALIDAÇÃO DO SISTEMA DE AQUISIÇÃO DE MEDIDAS

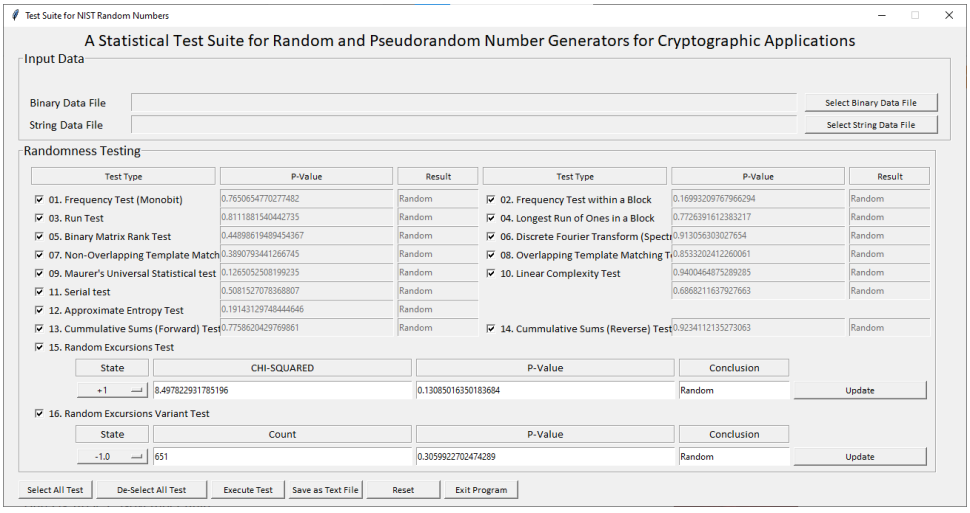
3.4.1 Validação da Ferramenta de Teste NIST e da Base de Dados de Referência:

A nossa solução requer a validação do processo de tratamento das medidas aleatórias. O primeiro passo para isso é a aquisição de uma base de dados verdadeiramente aleatória que será utilizada como referência. Nas etapas finais do estudo, as medidas obtidas no laboratório farão o papel que aqui será desempenhado pelo RTN sintético gerado a partir dessa base de dados de referência.

Essa base de dados será analisada pelo protocolo do NIST para validação de aleatoriedade. A ferramenta utilizada no presente estudo consiste na incorporação dos testes do protocolo em um software de código aberto (KHO ANG; CHURCHILL, 2022). Esses dados de referência serão, então, utilizando-se essa ferramenta, confirmados como verdadeiramente aleatórios. Esse processo também validará o próprio testador utilizado, já que temos como referência que esses dados são provenientes de fenômenos aleatórios. Como mencionado anteriormente, as medidas

escolhidas são oriundas de um gerador quântico (ANU QRNG, 2022). As medidas são oferecidas em tempo real, através de aquisições de blocos de 1025 bits. Para a validação de um número como aleatório, foi determinado, através de sucessivas análises, que é necessária uma sequência de, no mínimo aproximadamente 387840 (trezentos oitenta e seta mil e oitocentos e quarenta) bits. Sendo assim, foi desenvolvido um algoritmo de web scrapping para a aquisição e armazenamento de um conjunto de dados grande o suficiente para validação. A figura 11 mostra a validação de um conjunto de bits da nossa base de dados de referência, em que é possível verificar o resultado de cada um dos testes do NIST.

Figura 11 - Teste NIST de um conjunto de 399361 bits provenientes do gerador quântico



Fonte: Imagem de Elaboração Própria, software de autoria de (KHO ANG; CHURCHILL, 2022).

3.4.2 Sintetização de RTN

De posse dessa base de dados validada e aleatória, pode-se prosseguir para a próxima etapa de validação do nosso TRNG, a construção de um RTN sintético. Essa simulação de RTN alimentará o processo de simulação do nosso circuito gerador de números aleatórios, como se fosse a nossa base de dados medida.

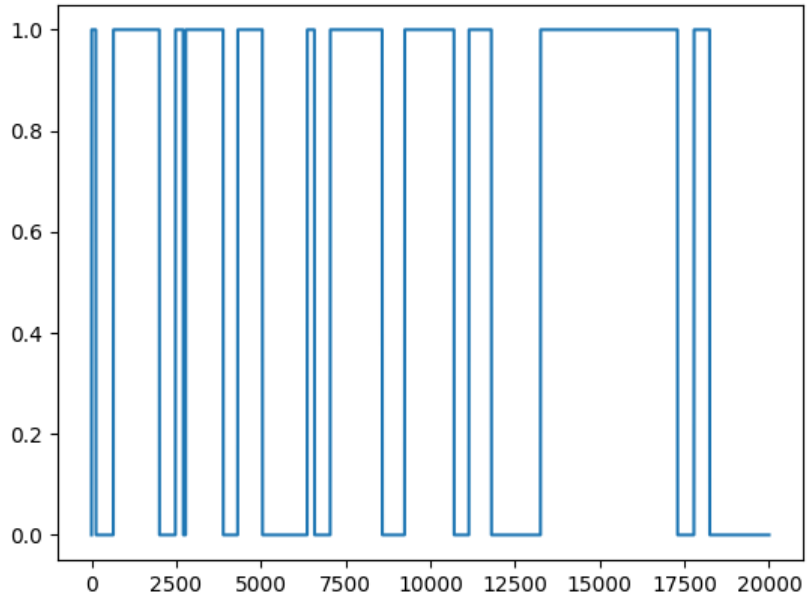
De uma forma um pouco mais específica, o processo para a simulação desse circuito gerador de números aleatórios a partir de RTN é bastante simples. Os valores

de entrada são o tempo de captura e emissão, isto é, os valores médios de tempo até a transição para cada um dos estados da armadilha de RTN, o conjunto de bits aleatórios previamente gerado e os valores de corrente para os dois estados de corrente.

Os bits aleatórios alimentarão o circuito de forma a servirem para determinar a transição ou não de um estado para outro. Os tempos de captura e emissão definem a probabilidade de transição e o número aleatório, a ocorrência dela.

Um vetor é então construindo, atribuindo-se o valor do estado, captura ou emissão, para cada índice, dependendo da ocorrência de transição ou não. A quantidade de pontos, que está relacionada ao tempo da medida, referente a permanência em cada estado é salva, excluindo-se os dois bits mais significativos.

Figura 12 - Exemplo de RTN sintetizado pelo algoritmo



Fonte: De autoria própria.

Conforme a imagem da figura 12, teremos então um RTN sintético, gerado através do conjunto de bits aleatórios previamente sintetizados. Para esse RTN em questão, foram utilizados tempos de captura e emissão médios iguais a 2500 pontos e valores de corrente iguais a 0 e 1. Para a geração de cada uma das probabilidades de transição, foram utilizados 10 bits do conjunto de dados. Os valores dos estados e a escala de tempo não são relevantes, já que o objetivo é apenas determinar a

aleatoriedade da medida sintetizada, contando-se o tempo de permanência em cada estado.

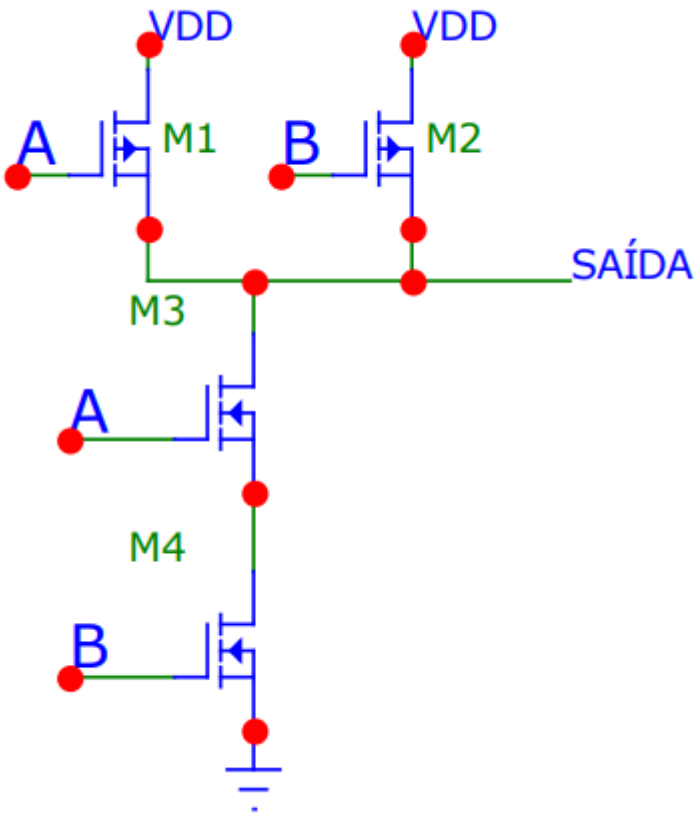
Após essa etapa de sintetização da medida, o conjunto de dados gerado, proveniente do tempo de permanência em cada um dos estados, é novamente submetido ao testador NIST e sua aleatoriedade é validada.

3.4.3 Simulação Spice do Contador De Tempo

Finalmente, serão validados a aquisição e interpretação da medida por um circuito eletrônico, determinando-se a ocorrência de possíveis fenômenos não aleatórios que comprometam a medida. No caso, foi desenvolvido um procedimento que alimenta uma simulação Spice de um contador de 8 bits, em nível de transistor, fornecendo como parâmetro de entrada os tempos do RTN, tanto de captura, quanto de emissão.

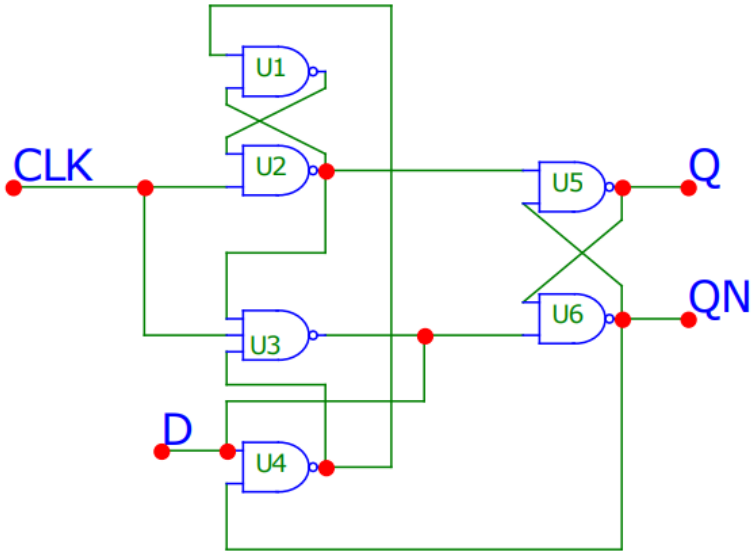
O circuito em questão é bastante simples, sendo um contador clássico de 8 bits, constituído por uma associação em cadeia de FLIP-FLOPS do tipo D, que por sua vez são construídos utilizando-se portas NAND, que, então, são constituídos por uma associação de transistores MOSFET.

Figura 13 - Subcircuito de porta NAND



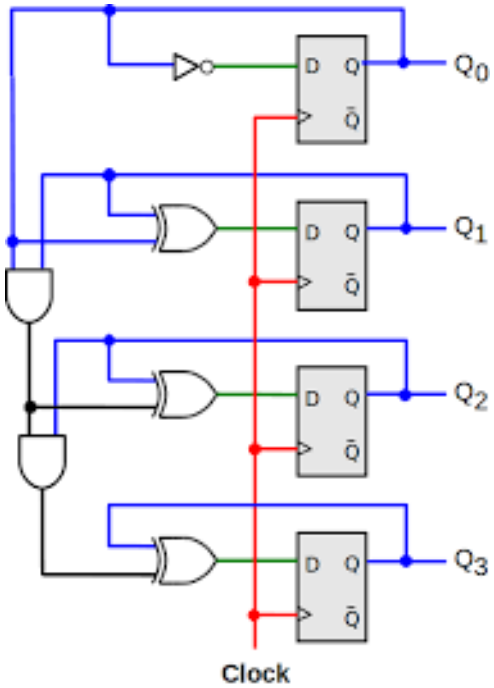
Fonte: De autoria própria.

Figura 14 - Subcircuito para a FLIP-FLOP D



Fonte: De autoria própria.

Figura 15 - Circuito final, com a associação dos subcirucitos de FLIPFLOP, AND e XOR



Fonte: Figura disponível em http://www.facom.ufms.br/~lianaduenha/sites/default/files/part07c.pdf. Acesso em 17 set. 2022.

Nas figuras 13, 14 e 15 é exibido o circuito de simulação Spice do contador de 8 bits. Ao final de cada transição do sinal de RTN, os valores armazenados nos 8 bits (Q0, Q1, ... Q7) do contador são salvos e uma nova contagem com um novo valor de tempo de captura ou emissão é iniciada. Depois de todos os tempos do RTN sintético terem sido processados pela simulação Spice, o arquivo gerado é analisado pelo testador NIST e sua aleatoriedade é atestada.

Ao final desse processo, a manutenção da aleatoriedade inicial da base de dados de referência é atestada e então a análise das medidas reais pode ser iniciada, que passará a fornecer nosso novo conjunto de dados que alimentará o circuito contador.

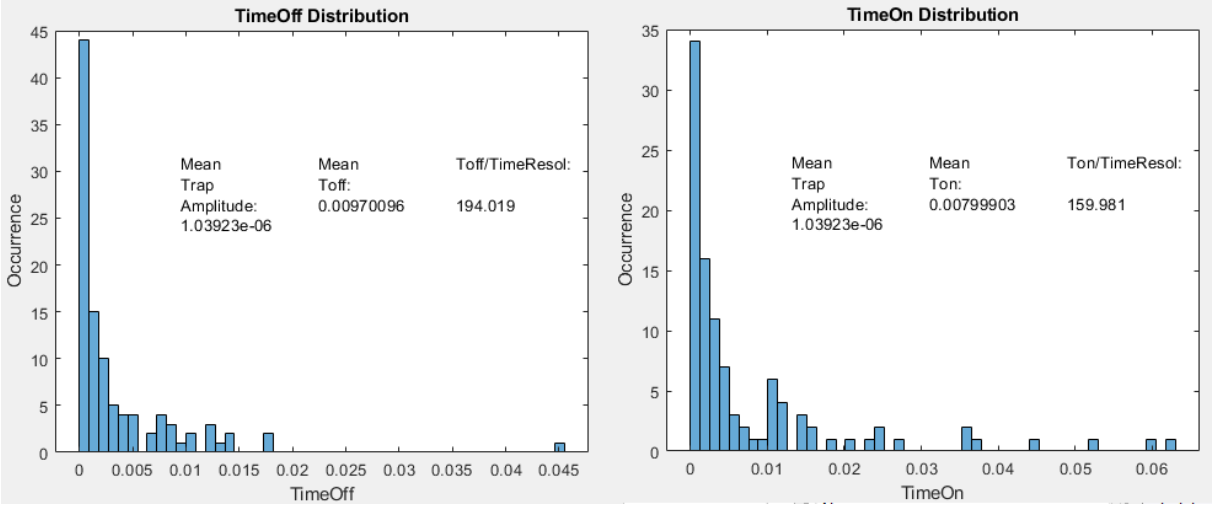
3.5 VALIDAÇÃO DA BASE DE DADOS OBTIDA NO LCE

A parte final do nosso estudo é a análise do conjunto de 430 medidas de RTN obtidas no laboratório de caracterização elétrica da UFRGS (LCE). Primeiramente é necessário, então, identificar a presença de RTN nas amostras e comprovar que o ruído observado realmente é o Random Telegraphic Noise.

Como características do RTN, temos suas transições discretas e seu perfil telegráfico, isto é, sem memória e aleatório na sua transição entre estados. Seu caráter aleatório fará com que os tempos de permanência em cada estado descrevam uma distribuição de Poisson. Considerando isso, podemos usar essas características como base para validar a presença de RTN nas amostras testadas.

Na figura 16 pode ser observado um exemplo da distribuição dos tempos de captura e emissão de uma das amostras. Há a presença de uma distribuição de Poisson no histograma da distribuição dos tempos, o que, conjuntamente com as outras características já mencionadas de RTN, determina a presença do ruído na amostra em questão.

Figura 16 – Distribuição dos Tempos de Captura (Time Off) e de Emissão (Time On) de uma medida exemplo



Fonte: De autoria própria.

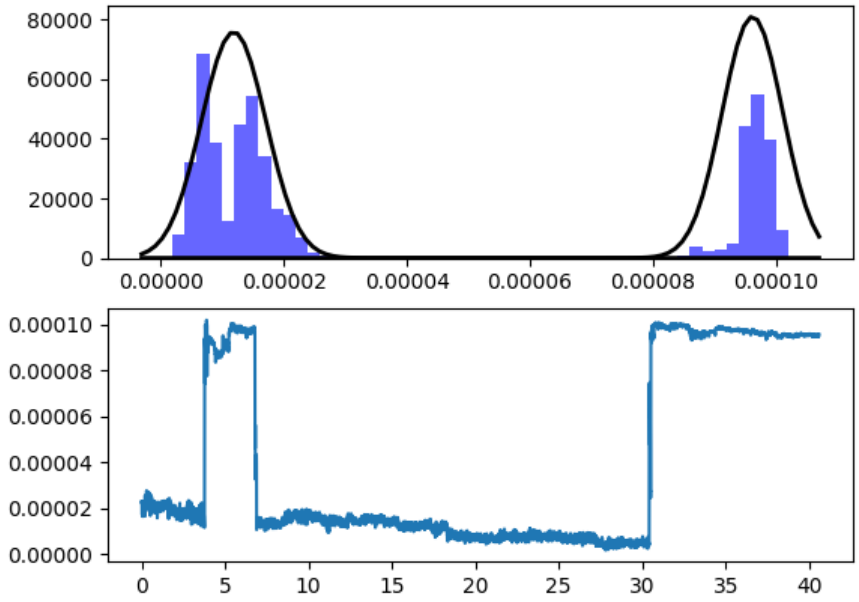
O desenvolvimento de um algoritmo que faça o processamento e a leitura dessas medidas é então necessário.

O objetivo do algoritmo desenvolvido é extrair os valores dos tempos de captura e emissão de cada uma das armadilhas presentes nas medidas. É importante salientar que diferentemente do RTN sintetizado, muitas medidas não apresentam somente uma armadilha atuante, de modo que o número de níveis de corrente é dado pela equação 1, onde N é o número de níveis de corrente em função de T, que é o número de armadilhas ativas.

$$N = 2^T \quad (1)$$

Sendo assim, o primeiro passo do nosso algoritmo de processamento de medidas será a identificação desses níveis de corrente, de modo a classificar discretamente cada ponto da medida como pertencente a um desses estados.

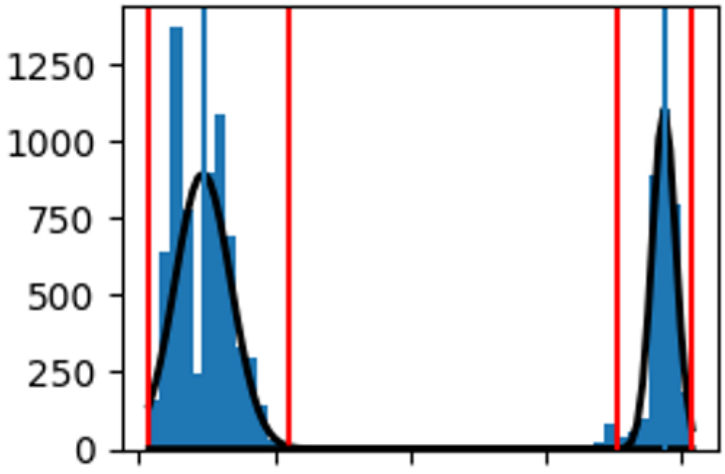
Figura 17 - Gráfico da medida HRS HBN com 14 V



Fonte: De autoria própria.

Como visto no gráfico da Figura 17, as medidas apresentam curvas gaussianas no histograma de corrente, sendo o centro de cada uma dessas curvas o valor médio de cada estado. A identificação dos diferentes estados pelo algoritmo se dará, então, pela identificação do intervalo das gaussianas e pela determinação do valor médio de corrente nesses intervalos.

Figura 18 - Histograma da medida com suas curvas gaussianas identificadas

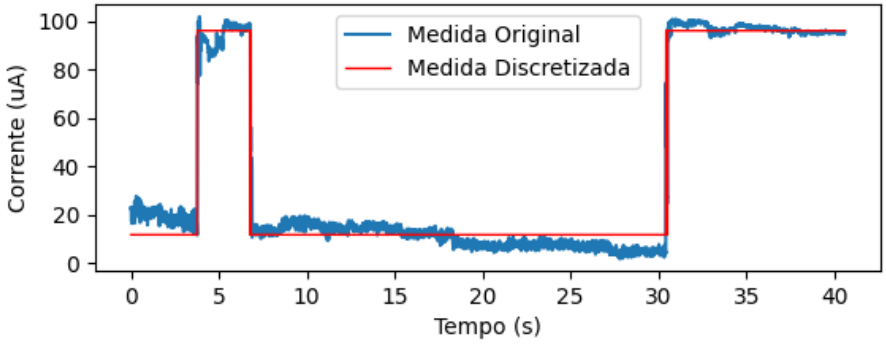


Fonte: De autoria própria.

Pelo gráfico da Figura 18, observamos a identificação e a determinação dos limites das gaussianas da medida original. O algoritmo em questão usa como base, para esses limites, os mínimos locais do histograma. O resultado é a identificação dos intervalos entre as linhas verticais vermelhas e a média de cada estado representado pela linha azul.

Uma vez identificadas as médias das Gaussianas, que serão os valores dos estados, é necessário determinar a qual deles cada um dos pontos da curva pertence. O critério de atribuição de cada ponto a um estado é o de menor distância absoluta. Esse processo é conhecido como discretização da medida, já que cada ponto só poderá assumir um valor discreto, isto é, um dos estados identificados pelo algoritmo. Na Figura 19 vemos essa discretização, sendo a linha vermelha a construção dessa medida discretizada e, a linha azul, a medida original.

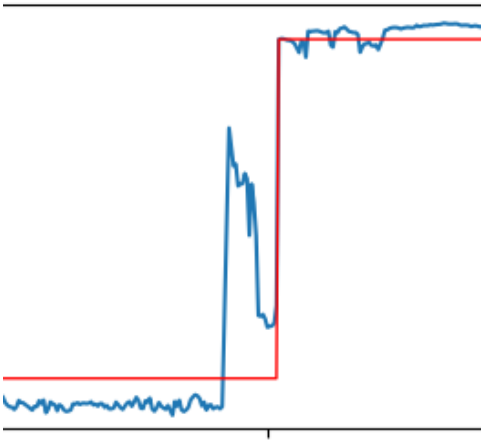
Figura 19 - Medida Discretizada



Fonte: De autoria própria.

A medida original apresenta alguns pontos indefinidos, ou seja, aqueles que estão entre dois estados. A proporção de pontos da medida que não se encaixam em nenhum estado discreto identificado é um indicador da qualidade da discretização. Essa grandeza será usada para indicar um possível aproveitamento da leitura da medida e o seu uso ou não na geração de números aleatórios. Na Figura 20, é possível perceber, antes da transição, esses pontos indefinidos. Nesse caso, o valor da medida discretizada é o mesmo do estado anterior.

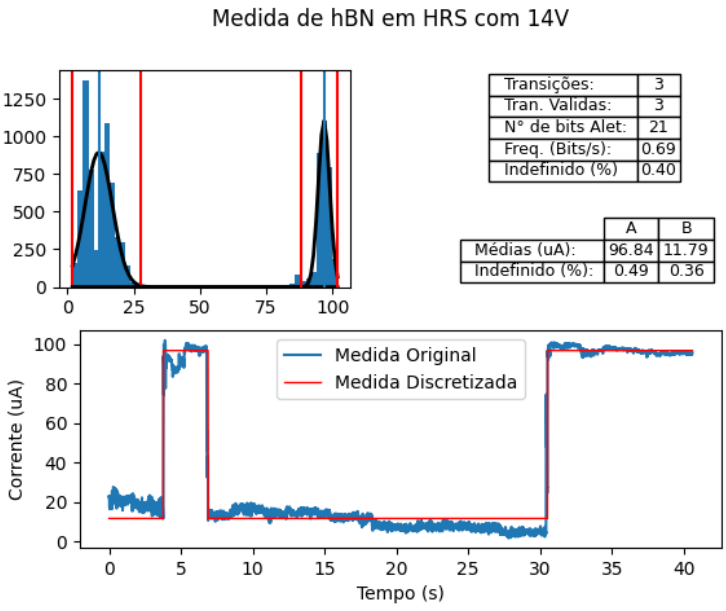
Figura 20 - Pontos Indefinidos da Medida



Fonte: De autoria própria.

Após a construção dessa medida discretizada e determinação de sua qualidade, os tempos de captura e emissão serão extraídos através de processo semelhante ao feito para o RTN sintético, produzindo um conjunto de bits, provenientes dos tempos de captura e emissão das armadilhas de RTN. Esses dados de saída das medidas serão novamente validados pelo teste NIST e a qualidade da sua aleatoriedade será avaliada.

Figura 21 - Sumarização do processamento da medida



Fonte: De autoria própria.

Pela imagem da Figura 21 é exposto, de uma forma resumida, o resultado do processamento da medida, executado pelo algoritmo desenvolvido. É possível verificar o número de transições, o número delas categorizado como válido (as quais levam a um estado com um tempo longo o suficiente para que a resolução da medição não impacte na determinação do tempo), o número de bits aleatórios gerados, a frequência de geração, e a porcentagem de pontos indefinidos, determinante da qualidade da discretização.

Depois de processadas todas as medidas da base de dados obtida, uma análise mais criteriosa do TRNG proposto será possível, avaliando-se peculiaridades no comportamento de cada semicondutor da base de dados (HBN, HFO e TIO2), o comportamento em cada estado de resistência (LRS e HRS) e a correlação desses fatores com a frequência de bits gerados.

4 RESULTADOS

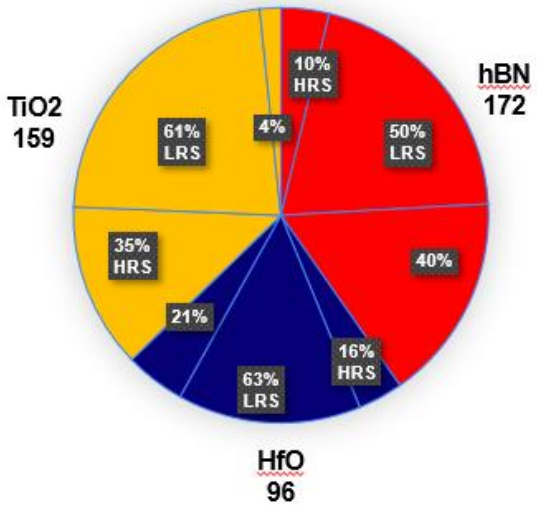
4.1 VALIDAÇÃO DO SISTEMA DE AQUISIÇÃO DE MEDIDAS

O sistema de aquisição de medidas (processo descrito na seção 3.2.), foi validado utilizando-se o NIST Test Suite, tendo como resultado a sua aleatoriedade atestada. Dessa forma, por meio de simulação Spice em nível de transistor, é validado que não há nenhuma degradação da medida original pelo processo de aquisição descrito.

4.2 VALIDAÇÃO DA BASE DE DADOS

A base de dados obtida no LCE tem 427 medidas, tendo a seguinte composição:

Figura 22 - Composição da base de dados adquirida

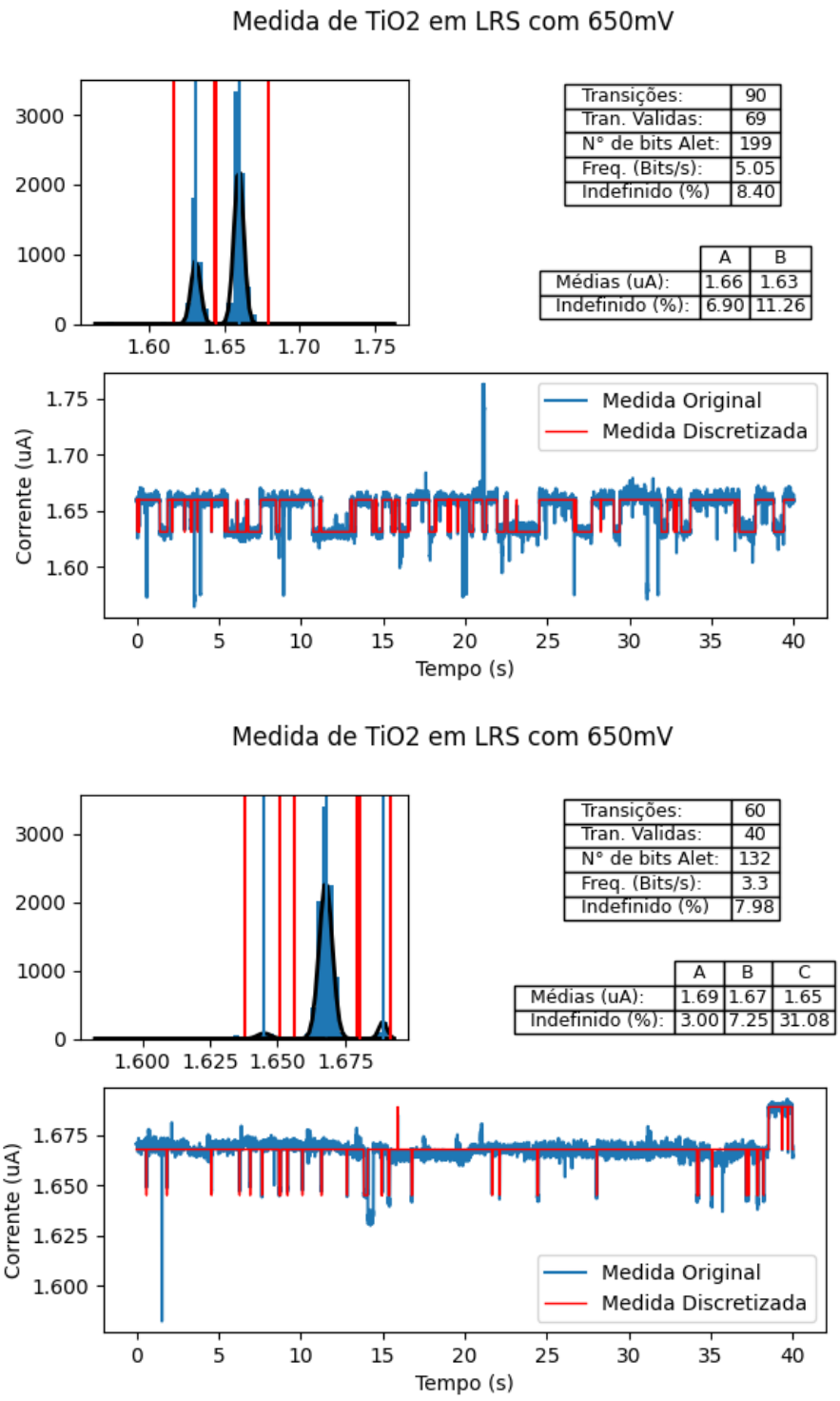


Fonte: De autoria própria.

O gráfico da Figura 22 mostra a base de dados analisada, com as diferentes amostras de memristores (TiO2, HfO e hBN) subdivididos pelos estados de resistência de cada medida (LRS, HRS e estado indefinido).

O algoritmo descrito na metodologia foi então usado para o processamento de nosso banco de dados. Das 427 medidas analisadas, 68 tiveram como resultado uma discretização de qualidade suficiente para a geração de números aleatórios (com as medidas escolhidas tendo, no máximo, 10% dos seus pontos em estado indefinidos e, também, tendo sido identificados no mínimo, dois estados de corrente).

Figura 23 - Exemplo de medidas selecionadas e processadas pelo algoritmo



Fonte: De autoria própria.

O processamento dessas medidas resultou em 2362 bits gerados, contendo a Figura 23 dois exemplos de medidas processadas . Esse conjunto de bits foi, então, submetido ao protocolo NIST para determinação de sua aleatoriedade.

Para a correta execução do protocolo, é necessário um conjunto de bits maior do que o gerado. Então foi utilizado o número aleatório de referência, selecionando-se apenas 2362 bits e comparando o resultado do NIST desse conjunto de referência, com o número gerado.

Tabela 1 - Resultados dos testes do NIST, para conjunto de bits gerado pelo banco de dados (Coluna Gerado) e a referência aleatória (Coluna Referência)

	Gerado	Referência
01. Frequency Test (Monobit)	Aleatório	Aleatório
02. Frequency Test within a Block	Aleatório	Aleatório
03. Run	Aleatório	Aleatório
04.Longest Run of Ones in a Block	Aleatório	Aleatório
05. Binary Matrix Rank	Aleatório	Aleatório
06. Discrete Fourier Transform	Aleatório	Aleatório
07. Non-Overlapping Template Match	Aleatório	Aleatório
08.Overlapping Template Matching	Aleatório	Aleatório
09. Maurer's Universal Statistical	Não Aleatório	Não Aleatório
10. Linear Complexity	Aleatório	Aleatório
11. Serial	Aleatório	Aleatório
12. Approximate Entropy	Não Aleatório	Não Aleatório
13. Cummulative Sums (Forward)	Aleatório	Aleatório
14. Cummulative Sums (Reverse)	Aleatório	Aleatório
15. Random Excursions	Aleatório	Aleatório
16. Random Excursions Variant	Aleatório	Aleatório

Fonte: De autoria própria.

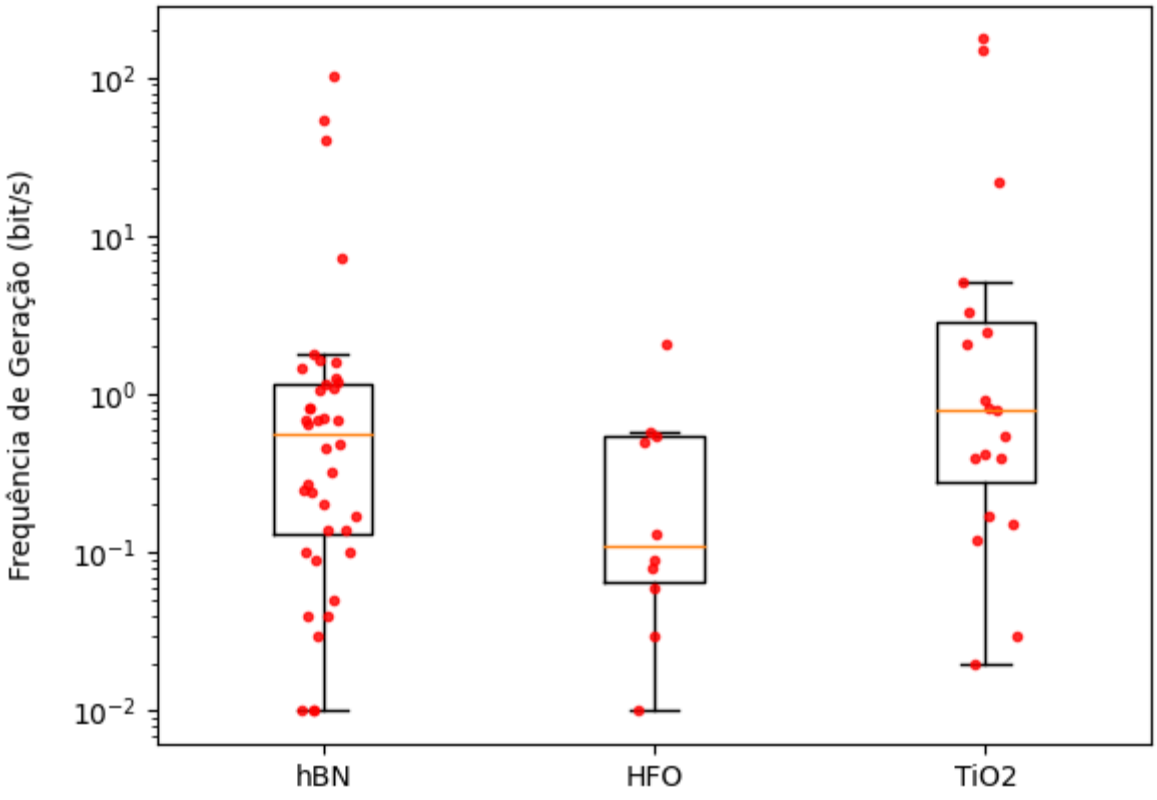
O mesmo resultado do NIST foi obtido para os conjuntos de bits gerado e de referência (que é verificado como aleatório). Sendo assim, há uma forte tendência de que a leitura e geração das medidas pelo algoritmo seja verdadeiramente aleatória.

4.2.1 Correlação entre Material Semicondutor e Frequência de Geração

Com a aleatoriedade dos números gerados comprovada, pode-se seguir à próxima etapa de interpretação dos dados gerados. Como afirmado anteriormente, uma das principais grandezas para determinação da qualidade de um TRNG é a frequência de geração de números aleatórios. Sendo assim, pode-se investigar uma possível correlação, utilizando-se como fatores os estados de resistência e o material semicondutor de cada amostra (hBN, TiO2, HfO), e sendo a variável de interesse a frequência de geração (bits/s).

Essa frequência de geração de cada uma das amostras foi obtida somando-se os bits gerados por cada uma das transições de RTN de uma medida específica e dividindo-se essa soma pelo tempo dessa medida. Dessa forma, cada uma das medidas que foram selecionadas tem uma frequência de geração associada, dada em bits/s.

Figura 24 - Diagrama de Caixa das medições por semicondutor utilizado



Fonte: De autoria própria.

Observa-se, pelo diagrama da Figura 24, as medições organizadas de acordo com o material semicondutor do memristor no qual a medição de RTN foi feita. Para determinar uma possível correlação entre esse semicondutor e a frequência de geração de números aleatórios, foi feita uma análise de variância (ANOVA). Essa análise de variância das médias dos diferentes grupos, aqui definidos pelo material semicondutor de suas células memristoras, revelou mais detalhes acerca do comportamento da frequência de geração dos números aleatórios em relação ao material das células das medidas. A ANOVA foi realizada utilizando-se o Excel, para um único fator, tendo os seguintes resultados:

Tabela 2 - Análise geral das medidas agrupadas por semicondutor

Grupo	Contagem	Soma	Média	Variância
hBN	40	223,01	5,58	348,99
HfO	10	4,12	0,412	0,40
TiO2	19	364,58	19,19	2593,23

Fonte: De autoria própria.

Tabela 3 - Análise de variância das medidas agrupadas por semicondutor

Fonte da variação	SQ	gl	MQ	F	valor-P	F crítico
Entre grupos	3166,54	2	1583,27	1,73	0,18	1,65
Dentro dos grupos	60292,30	66	913,52			

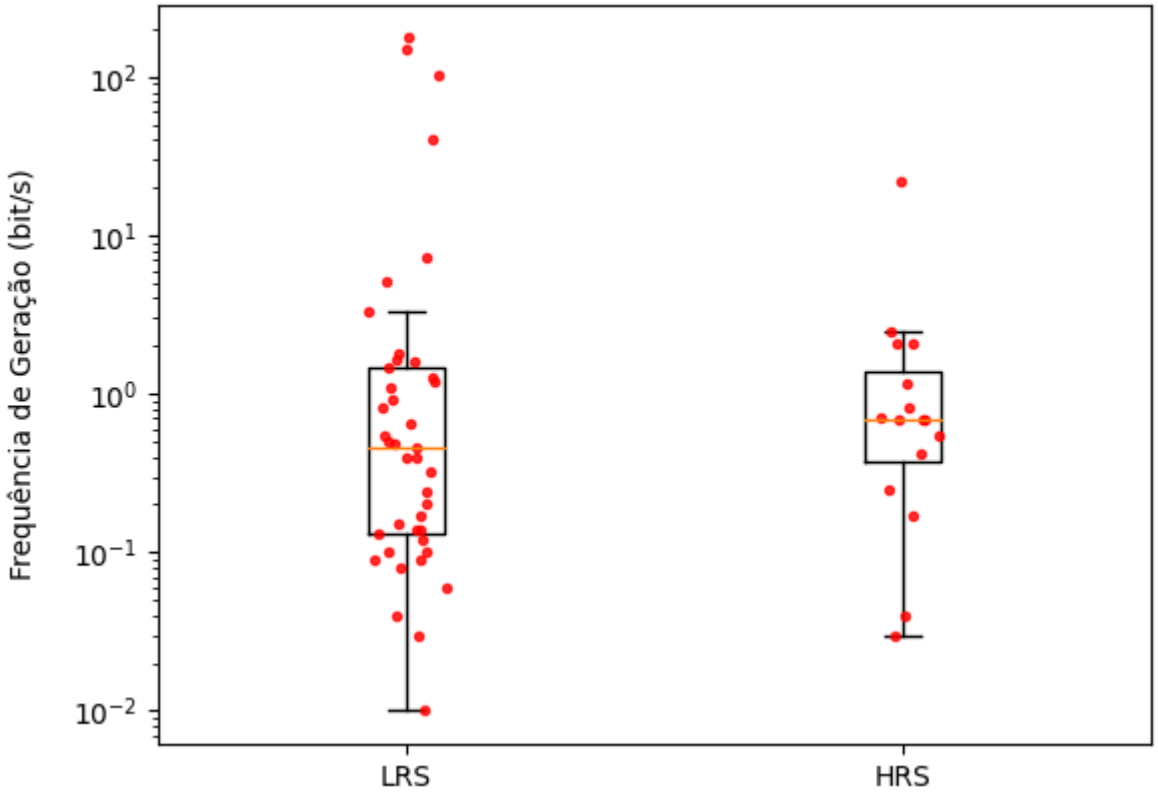
Fonte: De autoria própria.

A probabilidade de significância (valor-P) obtido foi de 0,18, pelo qual, utilizando-se um nível de significância (α) tradicional de 0,05, não é possível rejeitar a hipótese nula (H0). Contudo, considerando-se a grande variância e o número limitado de medidas, um valor-P de 0,18 é um bom indicativo de que realmente há uma correlação, tendo o dióxido de titânio, TiO2, uma média maior de geração de números aleatórios.

4.2.2 Correlação entre Estado de Resistência e Frequência de Geração

Considerando os diferentes níveis de resistência existentes em células memristoras, podemos repetir a análise da seção 4.2.1, utilizando como diferentes níveis os estados de resistência das medidas (hBN, TiO2, HfO).

Figura 25 - Diagrama de caixa das medições por estado de resistência



Fonte: De autoria própria.

Novamente, pela figura 25, temos as medidas organizadas em um diagrama de caixa, dessa vez utilizando-se como fatores os estados de resistência (LRS e HRS). Aplicou-se novamente a abordagem da seção anterior, realizando-se uma análise de variância (ANOVA). Dessa vez dividiu-se as amostras em grupos de estados de resistência, analisando-se a relação entre esse estado de resistência e a frequência de geração de bits aleatórios, obtendo-se os seguintes resultados:

Tabela 4 - Análise geral das medidas agrupadas por estado de resistência

Grupo	Contagem	Soma	Média	Variância
HRS	41	499,54	12,18	1476,70
LRS	16	34,93	2,18	28,57

Fonte: De autoria própria.

Tabela 5 - Análise de variância das medidas agrupadas por estado de resistência

Fonte da variação	SQ	gl	MQ	F	valor-P	F crítico
Entre grupos	1151,06	1	1151,06	1,06	0,31	1,68
Dentro dos grupos	59496,77	55	1081,76			

Fonte: De autoria própria.

A probabilidade de significância (valor-P) obtido dessa vez foi de 0,31, pelo qual, novamente, utilizando-se um nível de significância (α) de 0,05, não é possível rejeitar a hipótese nula (H0). Dessa vez, entretanto, obteve-se um valor-P significativamente maior, mesmo havendo mais amostras por nível e uma variância menor. Sendo assim, as chances de realmente haver uma correlação entre o estado de resistência e a frequência de geração são significativamente menores.

5 CONCLUSÃO

A partir do estudo desenvolvido, foi possível validar todas as etapas do sistema de aquisição do RTN, desde sua medição até o circuito contador. O procedimento de obtenção de números aleatórios a partir de RTN – que implementa o TRNG – e a base de dados foram analisados e a aleatoriedade dos números gerados foi atestada, certificando-se, assim, que o processamento das medidas preserva o caráter aleatório do RTN, demonstrando que o sistema de discretização é consistente com as medições reais.

A validação da metodologia desenvolvida abre, então, possibilidade para a análise dos dados obtidos. As análises de variância executadas para as influências

do material semicondutor e do estado de resistência na frequência de geração de bits aleatórios não permitiram a rejeição da hipótese nula. Contudo, houve uma indicação de que há maior potencial para criação de TRNG em células memoristoras de TiO2 em HRS, embora o estudo demonstre que seja possível construir tais dispositivos em todos os casos analisados.

Os resultados explicitam, então, que a construção de um dispositivo TRNG utilizando-se essas amostras e essa abordagem de contagem do tempo de cada estado de corrente é possível. O presente estudo fundamenta novos trabalhos que envolvam o aperfeiçoamento da abordagem desenvolvida e, também, a execução e construção do dispositivo propriamente dito.

REFERÊNCIAS BIBLIOGRÁFICAS

ABE, Kenichi *et al.* Anomalous Random Telegraph Signal Extractions from a Very Large Number of n-Metal Oxide Semiconductor Field-Effect Transistors Using Test Element Groups with 0.47 Hz–3.0 MHz Sampling Frequency. **Japanese Journal of Applied Physics**, [*s. l.*], v. 48, n. 4, p. 04C044, 2009.

BASSHAM, L E *et al.* **A statistical test suite for random and pseudorandom number generators for cryptographic applications**. Gaithersburg, MD: [*s. n.*], 2010.

BECKER, Thales *et al.* An Electrical Model for Trap Coupling Effects on Random Telegraph Noise. **IEEE Electron Device Letters**, [*s. l.*], v. 41, n. 10, p. 1596–1599, 2020.

BECKER, Thales *et al.* Resistive Switching Devices Producing Giant Random Telegraph Noise. **IEEE Electron Device Letters**, [*s. l.*], v. 43, n. 1, p. 146–149, 2022.

BREDERLOW, R. *et al.* A low-power true random number generator using random telegraph noise of single oxide-traps. *Em*: , 2006. **2006 IEEE International Solid State Circuits Conference - Digest of Technical Papers**. [*S. l.*]: IEEE, 2006. p. 1666–1675.

BROWN, James *et al.* A low-power and high-speed True Random Number Generator using generated RTN. *Em*: , 2018. **2018 IEEE Symposium on VLSI Technology**. [*S. l.*]: IEEE, 2018. p. 95–96.

CHAMPAGNE, Benoît; BISHOP, David M. Calculations of Nonlinear Optical Properties for the Solid State. *Em*: [*S. l.: s. n.*], 2003. p. 41–92.

HERRERO-COLLANTES, Miguel; GARCIA-ESCARTIN, Juan Carlos. Quantum random number generators. **Reviews of Modern Physics**, [*s. l.*], v. 89, n. 1, p. 015004, 2017.

KHO ANG, Stevven; CHURCHILL, Spence. **Randomness Test Suite**. [*S. l.*]: GitHub, 2022. Disponível em: https://github.com/stevenang/randomness_testsuite. Acesso em: 6 set. 2022.

NAGUMO, T. *et al.* New analysis methods for comprehensive understanding of Random Telegraph Noise. *Em*: , 2009. **2009 IEEE International Electron Devices Meeting (IEDM)**. [*S. l.*]: IEEE, 2009. p. 1–4.

NAGUMO, Toshiharu *et al.* Statistical characterization of trap position, energy, amplitude and time constants by RTN measurement of multiple individual traps. *Em*: , 2010. **2010 International Electron Devices Meeting**. [*S. l.*]: IEEE, 2010. p. 28.3.1-28.3.4.

ROHE, Markus; ADVISOR, Fortgeschrittenenpraktikum; ALKASSAR, Ammar. **RANDy-A True-Random Generator Based On Radioactive Decay**. [*S. l.: s. n.*], 2003.

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES. . Gaithersburg, MD: [*s. n.*], 2019.

THE AUSTRALIAN NATIONAL UNIVERSITY. **ANU QRNG (Australian National University Quantum Random Number Generator)**. [*S. l.*], [*s. d.*].

WIRTH, Gilson. Time Dependent Threshold Voltage Variability due to Random Telegraph Noise. *Em*: , 2020. **2020 IEEE Latin America Electron Devices Conference (LAEDC)**. [*S. l.*]: IEEE, 2020. p. 1–4.

WIRTH, Gilson; DA SILVA, Mauricio B.; BOTH, Thiago H. Towards Unifying the Statistical Modeling of Charge Trapping in Time and Frequency Domain. *Em*: , 2021. **2021 IEEE Latin America Electron Devices Conference (LAEDC)**. [*S. l.*]: IEEE, 2021. p. 1–3.