Geração de Sequências Pseudo-Aleatórias Baseadas no Mapa de Arnold Discreto Sobre $\mathbb{Z}_N$

Carlos E. C. Souza, Cecilio Pimentel e Daniel P. B. Chaves

***Resumo*— Neste trabalho é proposto um método para geração de sequências pseudo-aleatórias utilizando o mapa de Arnold sobre o anel de inteiros módulo N. É introduzida uma modificação no parâmetro de controle do mapa de Arnold discreto generalizado. O período das sequências geradas pelo método proposto é maior que o período obtido em outras propostas envolvendo mapas caóticos sobre anéis de inteiros. A análise da dinâmica do mapa de Arnold discreto é apresentada. O estudo da aleatoriedade de um gerador de números pseudo-aleatórios proposto neste trabalho é conduzido empregando-se a bateria de testes NIST, obtendo-se sucesso em todos.**

***Palavras-Chave*— Sequências pseudo-aleatórias, mapas caóticos, mapa de Arnold, caos discreto.**

***Abstract*— In this work we propose a method to generate pseudo random sequences based on the Arnold map over the integer ring. We introduce a modification in the control parameter of the generalized discrete Arnold map. The period of the generated sequences by the proposed method is longer than that of the sequences generated by another proposals based on chaotic maps over the integer ring. The dynamical analysis of the discrete Arnold map is presented. The analysis of the randomness of a proposed pseudo random number generator is conducted by employing the battery of tests NIST, being successful in all the tests.**

***Keywords*— Random sequences, chaotic maps, Arnold's map, discrete chaos.**

I. Introdução

Algumas características da dinâmica caótica, tais como sensibilidade às condições iniciais, comportamento recursivo e não periódico, espectro banda larga [1] evidenciam que mapas caóticos são potenciais candidatos para geradores de números pseudo-aleatórios (PRNG, *pseudo random number generators*) [2]–[7]. Quando estes mapas são definidos sobre os reais, os arredondamentos decorrentes das operações de ponto flutuante causam alterações na dinâmica original, devido à sensibilidade às condições iniciais [8]. A definição de mapas caóticos sobre espaços discretos é uma alternativa para evitar esta alteração pois as operações envolvidas são de ponto fixo, permitindo a reprodução exata da dinâmica.

Uma possível formalização do conceito de mapa caótico discreto é apresentada por Kocarev e Szczepanski em [9], [10]. Nestes trabalhos o conceito de caos discreto é definido e o expoente de Lyapunov é estendido para espaços discretos, sendo interpretado como a medida de dispersão média do sistema dinâmico discreto entre pontos vizinhos. O expoente de Lyapunov em espaços discretos é, analogamente ao caso contínuo, um indicativo de caos discreto quando possui valor positivo. No entanto, sistemas caóticos definidos sobre os reais são aperiódicos, uma propriedade que não ocorre em sistemas dinâmicos sobre espaços discretos, que geram sequências necessariamente periódicas. No entanto, apesar de serem periódicas, estas sequências são úteis para aplicações em PRNG, pois os seus períodos podem ser superiores à cardinalidade do conjunto discreto onde a sequência é definida. Recentemente surgiram novas propostas para geração de dinâmicas caóticas discretas. Em [11], [12] é analisado o período do mapa de Arnold sobre o anel de inteiros módulo N ($\mathbb{Z}_N$), sendo N a potência de um número primo. O mapa logístico sobre $\mathbb{Z}_N$ é investigado em [13].

Neste trabalho é proposto um método para geração de sequências unidimensionais baseado no mapa de Arnold definido sobre anéis de inteiros módulo N. Também é proposta uma modificação no mapa de Arnold generalizado com a introdução de um parâmetro de controle variável, com o objetivo de aumentar o período das sequências unidimensionais geradas. As sequências obtidas possuem período maior que as sequências do mapa logístico sobre $\mathbb{Z}_N$ proposto em [13]. A análise estatística realizada com a bateria de testes NIST [14] mostra que as sequências geradas pelo PRNG proposto passam em todos os testes, indicando que estas possuem um bom grau de aleatoriedade.

Este artigo está dividido em sete seções. Na Seção II é introduzido o mapa de Arnold, bem como suas versões discreta e generalizada. A geração de sequências unidimensionais baseadas no mapa de Arnold é detalhada na Seção III e é feita uma análise do período destas sequências. Na Seção IV é proposta uma modificação no parâmetro de controle do mapa de Arnold generalizado, com o objetivo de aumentar o período das sequências unidimensionais geradas. Na Seção V é discutido o conceito de caos em espaços discretos. A aplicação das sequências unidimensionais obtidas na construção de PRGNs é detalhada na Seção VI. Finalmente, na Seção VII, são apresentadas as considerações finais.

II. O Mapa de Arnold

O mapa de Arnold (ACM, *Arnold's cat map*) é um automorfismo toral definido por $\Gamma : \mathbb{R}^2/\mathbb{Z}^2 \to \mathbb{R}^2/\mathbb{Z}^2$ [15]

$$\Gamma(x, y) = (2x + y, x + y) \pmod 1 \tag{1}$$

em que $\mathbb{R}^2/\mathbb{Z}^2 = \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ é identificado com o toro bidimensional. O ACM é representado matricialmente por

$$\Gamma\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = A \begin{bmatrix} x \\ y \end{bmatrix} \pmod 1 \tag{2}$$

Carlos Souza, Departamento de Eletrônica e Sistemas - UFPE, e-mail: carlosecsouza@gmail.com; Cecilio Pimentel, Departamento de Eletrônica e Sistemas - UFPE, e-mail: cecilio@ufpe.br; Daniel Chaves, Departamento de Eletrônica e Sistemas - UFPE, e-mail: daniel.chaves@ufpe.br. Este trabalho foi parcialmente financiado por CNPq, FACEPE e CAPES.

em que

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}. \tag{3}$$

A dinâmica gerada pelo ACM é definida pela aplicação iterativa de Γ, isto é,

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod 1. \tag{4}$$

A iteração do ACM a partir de uma condição inicial (x_0, y_0) gera sequências bidimensionais $\{(x_0, y_0), (x_1, y_1), (x_2, y_2) \ldots\}$ tais que

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \pmod 1. \tag{5}$$

A matriz A possui autovalores $\lambda_\pm = (3 \pm \sqrt{2})/2$. Portanto, o maior expoente de Lyapunov do ACM $(\ln \lambda_+)$ é positivo, sendo um indicativo de comportamento caótico [16]. O determinante de A é igual a um, logo o ACM é um mapa que preserva áreas [16].

O mapa de Arnold é utilizado frequentemente em aplicações de segurança de imagens, como por exemplo em cifragem [17] e em marca d'água [18], pois é conveniente aplicar mapas bidimensionais nos pixels que compõem uma imagem. Este mapa é apresentado originalmente com a sua ação sobre a imagem de um gato [15], mostrando que ele gera um comportamento de *stretching* e *squeezing* [19] sobre esta, similarmente ao comportamento do conhecido mapa da ferradura de Smale [20].

O mapa de Arnold discreto (DACM, *Discrete Arnold's Cat Map*) é uma generalização do ACM para domínios discretos definido por $\Gamma_d : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$

$$\Gamma_d \left(\begin{bmatrix} x \\ y \end{bmatrix} \right) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N \tag{6}$$

em que $\mathbb{Z}_N$ é o anel de inteiros módulo N, $N = p^m$ e p é primo. Neste caso, o espaço de fase é um reticulado $N \times N$ sobre o toro bidimensional [8].

Na próxima seção, as sequências bidimensionais geradas pelo mapa Γ_d são transformadas em sequências unidimensionais com o objetivo de aplicação em PRNG e é feita uma análise computacional do período destas sequências.

III. Sequências Unidimensionais Geradas Pelo Mapa de Arnold

Definimos a sequência $\{z_n\} = \{z_0, z_1, z_2 \ldots\}$, $z_n \in \mathbb{Z}_N$ como

$$z_n = x_n y_n \pmod N \tag{7}$$

em que o par (x_n, y_n) é dado pela n-ésima iteração do mapa Γ_d. Esta sequência é dita ser periódica, com período T, quando $z_{i+T} = z_i$, $i \in \{0, 1, 2 \ldots\}$ e T é o menor valor para o qual esta condição é satisfeita. Para analisar o período de $\{z_n\}$ foram feitas buscas exaustivas para um dado conjunto $\mathbb{Z}_N$ com todas as possíveis condições iniciais (x_0, y_0). Consideramos $N = 3^m$, de forma equivalente ao mapa logístico sobre $\mathbb{Z}_N$ introduzido em [13]. Observa-se que o período de $\{z_n\}$ depende do valor de (x_0, y_0), havendo dois períodos possíveis:

- Quando x_0 e y_0 são ambos múltiplos de 3, o período é igual a $2N/27$.
- Caso contrário, o período é igual a $2N/3$, sendo este chamado de período máximo.

Por exemplo, considere a condição inicial $(x_0, y_0) = (1, 2)$ e $N = 3^3$. A sequência $\{z_n\}$ de período 18 (satisfazendo $T = 2N/3$) é (o início de cada período é destacado em negrito)

$$\{\mathbf{2}, \mathbf{12}, \mathbf{23}, 9, 8, 15, 11, 3, 5, 0, 17, 6, 20, 21, 14,$$
$$18, 26, 24, \mathbf{2}, \mathbf{12}, \mathbf{23}, \ldots\}.$$

As sequências geradas pelo mapa logístico sobre $\mathbb{Z}_N$ com $N = 3^m$ possuem período máximo igual a $N/3$ [13]. Logo o período máximo de $\{z_n\}$ é o dobro do período obtido com o mapa logístico considerando o mesmo conjunto $\mathbb{Z}_N$. Na próxima seção é proposta uma modificação mapa de Arnold discreto com o objetivo de aumentar o período máximo das sequências $\{z_n\}$.

IV. O Mapa Γ_v

Inicialmente, consideramos o mapa de Arnold discreto generalizado (GDACM, *Generalized Discrete Arnold's Cat Map*) definido em [21] por $\Gamma_g : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$

$$\Gamma_g \left(\begin{bmatrix} x \\ y \end{bmatrix} \right) = \begin{bmatrix} ab+1 & a \\ b & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N \tag{8}$$

em que $a, b \in \mathbb{Z}_N$ são parâmetros de controle e $N = p^m$. Escolhendo $a = b$ o mapa Γ_g possui um parâmetro e é escrito na forma

$$\Gamma_g \left(\begin{bmatrix} x \\ y \end{bmatrix} \right) = \begin{bmatrix} a^2+1 & a \\ a & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N. \tag{9}$$

Um problema tratado em [11], [12] é a análise de período de sequências bidimensionais geradas pelo mapa de Arnold discreto. Com o intuito de aumentar o período das sequências $\{z_n\}$, propomos uma modificação no mapa Γ_g substituindo o parâmetro a por um parâmetro variante que é incrementado em uma unidade a cada iteração. Desta forma, definimos o mapa $\Gamma_v : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$ por

$$\Gamma_v \left(\begin{bmatrix} x \\ y \end{bmatrix} \right) = \begin{bmatrix} n^2+1 & n \\ n & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N. \tag{10}$$

A dinâmica do mapa Γ_v é dada pela iteração

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} n^2+1 & n \\ n & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N. \tag{11}$$

Esta variação do parâmetro garante que mesmo quando um termo da sequência bidimensional é repetido, a sequência $\{z_n\}$ correspondente não entra em ciclo, possibilitando um aumento do período quando comparado ao das sequências geradas pelo mapa Γ_d.

Analogamente ao caso anterior, foram feitas buscas exaustivas para $\mathbb{Z}_N$ da forma 3^m com todas as possíveis condições iniciais para calcular o período das sequências geradas pelo mapa Γ_v. O período de $\{z_n\}$ também depende do valor de (x_0, y_0), com dois períodos possíveis:

- Quando x_0 e y_0 são ambos múltiplos de 3, o período é igual a $2N/9$.

- Caso contrário, o período é igual a $2N$, sendo este o período máximo.

O período máximo das sequências $\{z_n\}$ geradas por Γ_v é o triplo das sequências geradas por Γ_d. Utilizando a condição inicial $(x_0, y_0) = (1, 2)$ e $N = 3^3$, a sequência $\{z_n\}$ gerada pelo mapa Γ_v de período 54 é

$$\{\mathbf{2}, \mathbf{12}, \mathbf{16}, \mathbf{22}, \mathbf{18}, 23, 26, 18, 1, 19, 21, 17, 23, 15, 13, 16, 15, 11, 20, 12, 25, 13, 18, 5, 17, 18, 10, 10, 21, 26, 14, 15, 22, 7, 15, 20, 11, 12, 7, 4, 18, 14, 8, 18, 19, 1, 21, 8, 5, 15, 4, 25, 15, 2, \mathbf{2}, \mathbf{12}, \mathbf{16}, \mathbf{22}, \mathbf{18}, \ldots\}.$$

Observe que o quinto termo é igual a 18, e este mesmo termo ocorre na oitava posição, porém como o parâmetro é incrementado a cada iteração, a repetição de alguns termos não necessariamente implica que a sequência entra em ciclo.

Como a dinâmica caótica é um fenômeno característico do espaços contínuos, a generalização do ACM para conjuntos discretos não herda de forma direta as propriedades do comportamento caótico. Entretanto, algumas características da dinâmica discreta podem ser interpretadas como manifestações de caos. Para isso, é necessário estender o conceito de dinâmica caótica para o caso de espaços discretos. Na próxima seção é feita uma breve discussão sobre o conceito de caos discreto e são discutidas características de mapas definidos sobre espaços discretos.

V. Caos em Espaços Discretos

Em espaços contínuos, a sensibilidade às condições iniciais se manifesta pela separação exponencial entre trajetórias geradas por condições iniciais próximas [1]. A taxa de separação entre trajetórias é quantificada pelo expoente de Lyapunov, que quando tem valor positivo é um indicativo de comportamento caótico [1]. No entanto, mapas definidos em espaços discretos são necessariamente periódicos, portanto não existe caos no sentido tradicional em tais espaços [8].

O expoente de Lyapunov de mapas definidos em espaços discretos é proposto em [9] para analisar o comportamento de mapas caóticos definidos em espaços discretos, sendo este interpretado como a taxa de espalhamento local entre pontos vizinhos em sistemas dinâmicos discretos [10]. O conceito de vizinhança neste caso é entendido da seguinte forma: seja X uma sequência e x_n o n-ésimo ponto de X, então define-se os pontos x_{n-1} e x_{n+1} como vizinhos a x_n. Inicialmente, consideremos um mapa $F : \{0, 1, 2, \ldots, N-1\} \to \{0, 1, 2, \ldots, N-1\}$ sobre $\mathbb{Z}_N$. Segue que todas as trajetórias geradas por F são necessariamente periódicas. Seja $X = \{x_0, x_1 = F(x_0), \ldots, x_{T-1} = F(x_{T-2}), x_T = x_0\}$ uma sequência periódica com período T. O expoente de Lyapunov discreto da sequência X é definido em [9] por

$$\lambda_{(F,X)} = \frac{1}{T} \sum_{n=0}^{T-1} \ln |F(x_n + 1) - F(x_n)|. \qquad (12)$$

O expoente de Lyapunov discreto de F pode ser calculado pela soma ponderada dos expoentes de Lyapunov discretos de todas as sequências X_i periódicas geradas por F, ou seja

$$\lambda_F = \sum_i \frac{T_i}{M} \lambda_{(F,X_i)} \qquad (13)$$

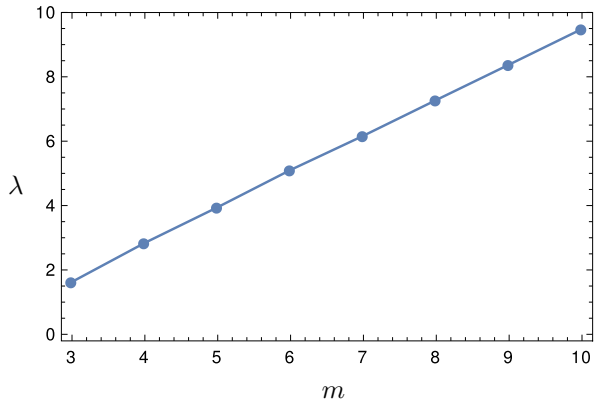

Fig. 1. Expoente de Lyapunov em função de m para $\{z_n\}$ gerada a partir de Γ_v com $N = 3^m$.

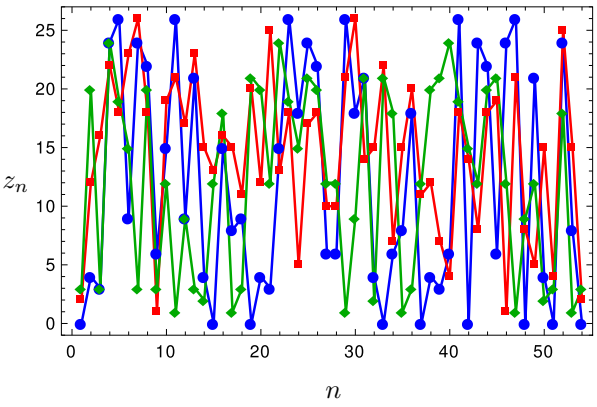

Fig. 2. Sequências $\{z_n\}$ geradas pelo mapa Γ_v sobre $\mathbb{Z}_{33}$ com condições iniciais vizinhas $(0, 2)$, $(1, 2)$ e $(1, 3)$. O período das sequências é $T = 54$.

em que T_i é o período de X_i. Quando λ_F é positivo, o mapa F possui comportamento de caos discreto, também denominado de pseudo-caótico [10]. No caso particular em que o mapa discreto é obtido a partir de uma quantização adequada de um mapa caótico real, o expoente de Lyapunov discreto tende ao expoente do Lyapunov do mapa real no limite em que $M \to \infty$.

O expoente de Lyapunov calculado para $\{z_n\}$ geradas por Γ_v com $N = 3^m$ em função de m, é ilustrado na Fig. 1. O valor do expoente cresce com o valor de m, sendo sempre positivo, indicado que existe um comportamento de caos discreto. A Fig. 2 ilustra a evolução da sequência $\{z_n\}$ gerada pelo mapa Γ_v com três condições iniciais vizinhas, mostrando que as sequências apresentam um comportamento de dispersão no conjunto $\mathbb{Z}_N$.

A entropia aproximada (ApEn, *Approximate Entropy*) foi introduzida em [22] para avaliar a regularidade de uma sequência. Em [23], a ApEn é utilizada para analisar o comportamento de sequências geradas por mapas caóticos. A ApEn é calculada particionando-se a sequência em blocos e calculando-se a máxima distância relativa entre os elementos de dois blocos para todos os blocos. O parâmetro r é um limiar utilizado para avaliar a proximidade entre blocos. A ApEn máxima é obtida tipicamente quando r é escolhido entre $0{,}1$ e

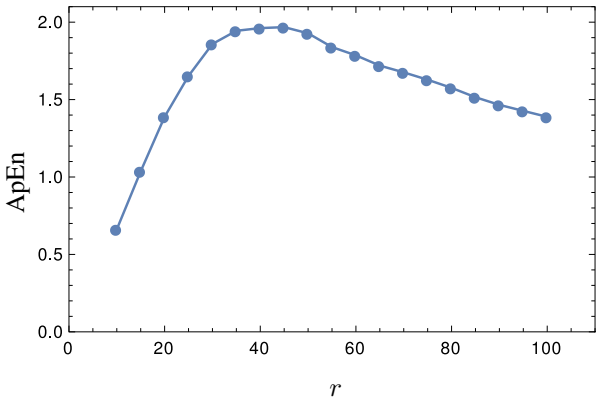

Fig. 3. Entropia aproximada para o mapa Γ_v em função do parâmetro r com $N = 3^6$.

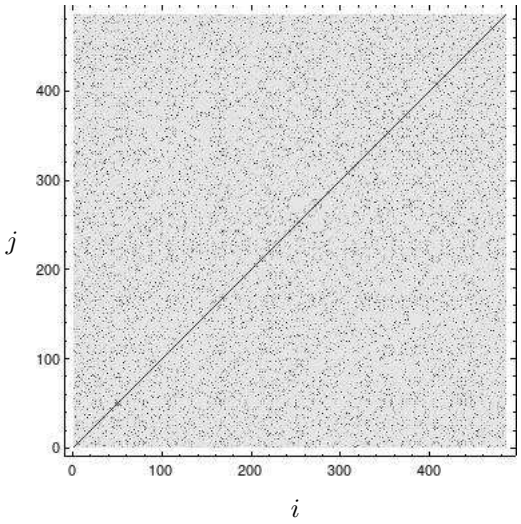

Fig. 4. Gráfico de recorrência para as sequências $\{z_n\}$ geradas pelo mapa Γ_v para $N = 3^5$.

0,2 vezes o desvio padrão da sequência. No caso de sequências regulares a ApEn máxima se aproxima de zero. A Fig. 3 mostra a ApEn para uma sequência $\{z_n\}$ gerada por Γ_v com $N = 3^6$ em função do parâmetro r. Como a ApEn máxima é aproximadamente dois, então a sequência $\{z_n\}$ apresenta características de aleatoriedade.

Outra forma de analisar o comportamento de sistemas dinâmicos é o gráfico de recorrência, (RP, *recurrence plot*), introduzido em [24]. O RP para uma sequência de pontos $\{z_n\}$ indica para cada ponto z_i de $\{z_n\}$ se existem pontos z_j numa vizinhança de z_i satisfazendo $|z_i - z_j| \leq \varepsilon$, em que ε é o raio da bola com centro em z_i. Quando a sequência é aleatória, o RP ocupa uniformemente toda a região, sem apresentar padrões ou alta concentração de pontos em sub-regiões. A Fig. 4 mostra o RP para uma sequência $\{z_n\}$ gerada pelo mapa Γ_v com $N = 3^5$. Escolhemos $\varepsilon = 5$, de forma que uma vizinhança para um ponto de $\{z_n\}$ com período igual a $2N$ tem raio aproximadamente igual a 1% do comprimento da sequência. O RP mostra que as sequências $\{z_n\}$ geradas pelo mapa Γ_v não apresentam padrões ou concentração de pontos, indicando que são sequências com comportamento similar ao de sequências aleatórias.

VI. Aplicação: PRNG

Nesta seção, as sequências $\{z_n\}$ são aplicadas na construção de PRNGs. Inicialmente, estas são mapeadas em sequências binárias. Para isto, cada elemento de $\{z_n\}$ é representado em forma binária. Em seguida, o bit menos significativo de cada elemento é extraído, o que equivale à redução módulo dois, e estes bits são empregados para construir uma sequência binária a partir de $\{z_n\}$. As propriedades estatísticas do mapa proposto foram analisadas com o bateria de testes NIST versão SP800-22 [14].

A bateria de testes NIST é um conjunto de 15 testes estatísticos baseados em testes de hipóteses, desenvolvidos para analisar a aleatoriedade de sequências binárias. Cada teste determina a aceitação ou rejeição da hipótese que detecta desvios da aleatoriedade da sequência testada. A bateria NIST fornece como resultado a proporção de subsequências aprovadas nos testes. Cada teste é calculado com nível de confiança α e o valor recomendado em [14] é $\alpha = 0{,}01$. Foram utilizadas 1000 subsequências binárias sendo cada uma de comprimento 10^6. Para este valor de α e 1000 subsequências, cada teste é aprovado quando a proporção de subsequências aprovadas é no mínimo 0,980.

TABELA I

Resultados do bateria de testes NIST para as sequências $\{z_n\}$ geradas pelos mapas Γ_n, Γ e para as sequências geradas pelo mapa logístico com $N = 3^m$ em todos os casos. Os resultados em negrito indicam que o teste não foi aprovado.

Statistical test	Γ_v	Γ_d	Log.
Frequency	0,988	0,989	0,985
BlockFrequency	0,990	0,987	0,990
CumulativeSums Min.	0,986	0,990	0,984
CumulativeSums Max.	0,990	0,993	0,986
Runs	0,994	0,990	0,987
LongestRun	0,993	**0,975**	0,992
Rank	0,990	0,992	0,990
FFT	0,988	0,984	0,988
Non-Ovla. Temp. Min.	0,982	**0,958**	0,980
Non-Ovla. Temp. Max.	0,998	0,998	0,998
Ovla. Temp.	0,986	**0,932**	0,991
Universal	0,989	0,991	0,988
ApproximateEntropy	0,987	**0,846**	0,989
Ran. Exc. Min.	0,982	0,982	0,980
Ran. Exc. Max.	0,994	0,995	0,992
Ran. Ex. Var. Min.	0,985	0,981	0,985
Ran. Ex. Var. Max.	0,994	0,995	0,994
Serial Min.	0,987	**0,978**	0,984
Serial Max.	0,994	0,985	0,990
LinearComplexity	0,992	0,988	0,990

A Tabela I mostra os resultados obtidos para as sequências binárias geradas a partir dos mapas Γ_d e Γ_v pela aplicação de (7), e as sequências geradas pelo mapa logístico, todos definidos em $\mathbb{Z}_N$ com $N = 3^m$. O valor de m é escolhido de acordo com o mapa, de forma que o período da sequência seja no mínimo 10^9. Alguns testes são múltiplos, como por exemplo o *non-overlapping template. Nestes casos apresentamos a proporção mínima e máxima.* As sequências

geradas com o mapa Γ_v apresentam sucesso nos 15 testes do NIST, enquanto o mapa Γ_d falha em cinco testes, indicados em negrito, mostrando que a modificação introduzida no parâmetro de controle resulta em melhor aleatoriedade. As sequências geradas pelo mapa logístico também passam em todos os testes, porém na maioria dos casos apresentando proporções menores que as das sequências geradas pelo mapa Γ_v, além de terem período seis vezes menor.

VII. Conclusões

PRNGs são essenciais para a implementação de sistemas criptográficos. Quando se utiliza mapas caóticos definidos sobre os reais, os arredondamentos da operação de ponto flutuante interfere na dinâmica caótica [8]. Uma alternativa para contornar este problema é definir tais sistemas em anéis de inteiros. Neste trabalho, foi apresentado um método para geração de sequências unidimensionais com a utilização do mapa de Arnold sobre anéis de inteiros módulo N para aplicação em PRNGs. Foi introduzida uma modificação no parâmetro do mapa de Arnold discreto generalizado. Além de passar na bateria de testes do NIST, o método proposto gera sequências binárias com período maior que as sequências geradas pelo mapa logístico sobre o mesmo anel de inteiros. Portanto, a proposta se mostra viável, apresentando algumas vantagens em relação a sistemas semelhantes introduzidos recentemente na literatura.

Referências

[1] S. Strogatz, *Nonlinear Dynamics and Chaos with Applications to Physics, Biology, Chemistry, and Engineering*, ser. Studies in Nonlinearity Series. Westview Press, 2001.

[2] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators. Part II: practical realization," *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.*, vol. 48, no. 3, pp. 382–385, Mar. 2001.

[3] T. Stojanovski and L. Kocarev, "Chaos-based random number generators-part I: analysis [cryptography]," *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.*, vol. 48, no. 3, pp. 281–288, Mar. 2001.

[4] A. Beirami and H. Nejati, "A framework for investigating the performance of chaotic-map truly random number generators," *IEEE Trans. Circuits and Syst. II: Exp. Briefs*, vol. 60, no. 7, pp. 446–450, July 2013.

[5] R. A. Elmanfaloty and E. Abou-Bakr, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation," *Chaos, Solitons & Fractals*, vol. 118, pp. 134 – 144, jan. 2019.

[6] M. Garcia-Bosque, A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, and S. Celma, "Chaos-based bitwise dynamical pseudorandom number generator on FPGA," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 1, pp. 291–293, Jan. 2019.

[7] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1273–1284, Feb. 2019.

[8] B. Chirikov and F. Vivaldi, "An algorithmic view of pseudochaos," *Physica D: Nonlinear Phenomena*, vol. 129, no. 3, pp. 223 – 235, May 1999.

[9] L. Kocarev and J. Szczepanski, "Finite-space Lyapunov exponents and pseudochaos," *Phys. Rev. Lett.*, vol. 93, p. 234101, Dec. 2004.

[10] L. Kocarev, J. Szczepanski, J. M. Amigo, and I. Tomovski, "Discrete chaos-I: Theory," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 6, pp. 1300–1309, June 2006.

[11] F. Chen, K. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold cat map for $N = p^e$," *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 445–452, Jan 2012.

[12] ——, "Period distribution of the generalized discrete Arnold cat map for $N = 2^e$," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 3249–3255, May 2013.

[13] B. Yang and X. Liao, "Some properties of the logistic map over the finite field and its application," *Signal Processing*, vol. 153, pp. 231 – 242, Dec. 2018.

[14] L. E. B. III *et al.*, *SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Gaithersburg, MD, United States: Nat. Inst. Std. & Technol., 2010.

[15] V. Arnold and A. Avez, *Ergodic Problems of Classical Mechanics*. New York:Benjamin, 1968.

[16] B. H. Anatole Katok, *Introduction to the Modern Theory of Dynamical Systems*, ser. Encyclopedia of Mathematics and its Applications 54. Cambridge University Press, 1995.

[17] M. Farajallah, S. El Assad, and O. Deforges, "Fast and secure chaos-based cryptosystem for images," *International Journal of Bifurcation and Chaos*, vol. 26, no. 02, p. 1650021, 2016.

[18] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," *IEEE Access*, vol. 6, pp. 19 876–19 897, Mar. 2018.

[19] R. Gilmore and M. Lefranc, *The Topology of Chaos: Alice in Stretch and Squeezeland*, 2nd ed. Wiley-VCH, 2012.

[20] S. Smale, "Differenciable dynamical systems," *Bull. Am. Math. Soc.*, vol. 73, pp. 747–817, 1967.

[21] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749 – 761, July 2004.

[22] S. M. Pincus, I. M. Gladstone, and R. A. Ehrenkranz, "A regularity statistic for medical data analysis," *Journal of Clinical Monitoring*, vol. 7, no. 4, pp. 335–345, Oct. 1991.

[23] Z. Li, J. Cai, and Y. Chang, "Determining the complexity of FH/SS sequence by approximate entropy," *IEEE Transactions on Communications*, vol. 57, no. 3, pp. 812–820, March 2009.

[24] J.-P. Eckmann, S. O. Kamphorst, and D. Ruelle, "Recurrence plots of dynamical systems," *Europhysics Letters (EPL)*, vol. 4, no. 9, pp. 973–977, nov. 1987.