Uma Metodologia para Geração de Sequências Aleatórias usando Mapas Caóticos

José A. P. Artiles, Daniel P. B. Chaves, João V. C. Evangelista e Cecilio Pimentel

***Resumo*— Geradores de números aleatórios são amplamente utilizados em aplicações científicas e tecnológicas. Particularmente em criptografia, são empregados em sistemas de chave pública, assinatura digital. Neste trabalho, apresentamos uma metodologia para o projeto destes geradores a partir de mapas caóticos baseada em duas técnicas: salto de amostras e discretização codificada variante no tempo. Mostramos que o procedimento possui alta taxa de geração de bits, além de dispensar pós-processamento para melhoria de suas propriedades aleatórias. Validamos o método proposto empregando o teste NIST. Por fim, apresentamos um circuito que implementa o mapa caótico analisado neste trabalho.**

***Palavras-Chave*— Mapas caóticos, sistemas dinâmicos, geração de números aleatórios, taxa de entropia, teste NIST.**

***Abstract*— Random number generators are widely used in scientific and technological applications. Particularly in cryptography, they are employed in public key systems and digital signature. This work presents a methodology for the design of these generators from chaotic maps based on two techniques: Skipping and time-varying coded discretization. We show that the proposed method has high bit generation rate and dispenses post-processing in order to improve their random properties. The effectiveness of this procedure is verified through the NIST test. Finally, we present a circuit implementation of the chaotic map considered in this work.**

***Keywords*— Chaotic maps, dynamical systems, random numbers generator, entropy rate, NIST test.**

I. Introdução

As propriedades inerentes aos sistemas dinâmicos caóticos, como a dependência às condições iniciais, o comportamento pseudoaleatório e o espectro faixa larga, por vezes evocadas para sua caracterização [1], [2], reservam similaridade com as funções requeridas por alguns blocos de um sistema de comunicação clássico. Nos anos 90 surgiram novas concepções de sistemas de comunicação [3] que propuseram o aproveitamento dessas propriedades para transmissão de informação de forma eficiente. Desde então, diversos trabalhos científicos propiciaram o amadurecimento da área, demonstrando a vocação de sistemas caóticos para compressão de dados [4], [5], modulação [6], [7], [8] e criptografia [9], [10].

Em decorrência da diversidade de sistemas caóticos, sua aplicação em criptografia é ubíqua, sendo utilizado em sistemas criptográficos de chave privada, geradores de números pseudo-aleatórios (PRNG, *pseudo-random number generator*), e sistemas criptográficos de chave pública [9], [11]. Contudo, certas aplicações em criptografia requerem o emprego de geradores de números aleatórios (RNG, *random number generator*). Neste caso, o núcleo do RNG deve ser um processo físico inerentemente aleatório, o que limita consideravelmente sua aplicação, como consequência da dificuldade técnica em implementa-lo. Como alternativa, os sistemas caóticos podem ser considerados como RNG's quando, apesar de sua natureza determinística se definidos sobre o conjuntos dos números reais, forem "observados" através de sequências discretas de símbolos, gerados a partir de uma partição finita do seu espaço de fase [12]. Isso equivale a empregar a dinâmica simbólica associada ao sistema, ao invés de uma sequência de números reais obtida pela interação do mapa que define o sistema caótico.

A despeito da complexidade das sequências geradas a partir de sistemas caóticos, esses são muitas vezes de baixa dimensão e definidos por recursões simples. No entanto, como decorrência da estrutura inerente aos sistemas dinâmicos, as propriedades estatísticas das sequências obtidas diretamente dos sistemas caóticos precisam comumente ser incrementadas para que possam ser atribuídas a um RNG. Em [13], três classes de quantificadores para essas propriedades são listadas: (i) baseados em teoria da informação, (ii) baseados em gráficos de recorrência, e (iii) baseados em técnicas computacionais. Os quantificadores propostos visam avaliar basicamente a uniformidade da distribuição invariante do sistema caótico e a independência entre iterações do mapa [13] que podem ser melhorados significativamente por técnicas de randomização de dinâmica simbólica [14].

Duas técnicas adotadas para geração de sequências aleatórias a partir de mapas caóticos são a discretização e o salto de amostras [14]. A análise destas sequências demonstra que o discretização atua tanto na uniformização da distribuição invariante quanto na redução de correlação. Já o salto de amostras só atua na redução de correlação, mantendo a distribuição invariante inalterada. Contudo, a redução da correlação é bem mais contundente ao emprego-se o salto de amostras que a discretização [14], [13]. A entropia condicional constitui um meio para verificar a eficácia destas técnicas, já que indica a uniformidade da distribuição invariante e a correlação da sequência [15]. De fato, a entropia condicional pode ser interpretada como um quantificador único que reflete propriedades estatísticas das sequências, servindo como guia para adoção de estratégias que melhorem estas propriedades.

Neste trabalho demonstramos como a entropia condicional pode ser empregada no projeto de RNG's com alta taxa de bits por amostra. Nesse contexto, listamos três contribui-

J. A. P. Artiles, D. P. B. Chaves, J. V. C. Evangelista e C. Pimentel, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, Brasil, E-mails: joseantonio.artiles@ufpe.br, daniel.chaves@ufpe.br, cecilio@ufpe.br. Este trabalho foi parcialmente financiado pelo CNPq e pela FACEPE.

ções principais. Inicialmente, demonstramos como empregar a entropia condicional para determinar o limiar inferior do salto de amostras para a quebra da correlação na sequência. Como segunda contribuição, especificamos como particionar o espaço de fase, além disso, como os respectivos intervalos devem ser codificados para garantir a distribuição uniforme de probabilidade da sequência gerada. Denominamos esta técnica de discretização codificada variante no tempo. Mostramos que, em conjunto, essas técnicas dispensam o emprego de unidades subsequentes de pós-processamento da sequência de bits, já que atingem a máxima taxa de entropia. Para testar a aleatoriedade das sequências geradas empregamos a versão 800-22 do teste NIST. Apesar do método considerado independer do mapa caótico, empregamos para estudo de caso o mapa stanh [16]. Por fim, apresentamos uma implementação eletrônica deste mapa e mostramos a aderência entre a curva característica do circuito e a obtida através do mapa teórico.

O artigo está organizado em sete seções. Na Seção II descrevemos o mapa stanh e suas propriedades estatísticas relevantes para este trabalho. Na Seção III a entropia condicional é introduzida como quantificador para avaliar a aleatoriedade das sequências e discutimos o seu emprego no projeto de RNG's. Na Seção IV descrevemos o processo de discretização codificada variante no tempo. Na Seção V avaliamos o RNG proposto através do teste NIST. Na Seção VI apresentamos uma possível implementação do mapa stanh empregando transistores de junção bipolar. Na Seção VII tecemos as conclusões deste trabalho.

II. O Mapa Caótico

Dada uma condição inicial x_0 e um mapa caótico unidimensional $f(x)$ forma-se uma série temporal através da iteração

$$x_n = f(x_{n-1}), \quad n = 1, 2, \ldots \tag{1}$$

Denomina-se $\{x_n\}_{i=0}^{\infty} = \{x_0, f(x_1), f(x_2), \ldots\}$ uma órbita de f iniciando em x_0. O mapa $f : [-1, 1] \to [-1, 1]$ usado neste trabalho, denominado de stanh, introduzido originalmente em [16], é baseado na função tangente hiperbólica e pode ser definido por

$$f(x) = \begin{cases} e \cdot \tanh\left(\frac{r}{1+\alpha} \cdot (x+1)\right) - 1, & x < \alpha \\ (-1)^b \cdot \left[e \cdot \tanh\left(-\frac{r}{1-\alpha} \cdot (x-1)\right) - 1\right], & x \geq \alpha \end{cases} \tag{2}$$

em que o fator de escala e é dado por

$$e = \frac{2}{\tanh(r)}. \tag{3}$$

Este mapa tem três parâmetros de controle especificados pela tripla (b, r, α). O parâmetro b define a simetria do mapa, podendo ser 0 (simetria par) ou 1 (simetria ímpar). O parâmetro $\alpha \in (-1, 1)$ estabelece o eixo de simetria (dado por $x = \alpha$), este é deslocado para direita se $\alpha > 0$ ou para esquerda se $\alpha < 0$. O parâmetro r é um número real positivo que controla a extensão da região planar em torno do eixo de simetria. Neste trabalho assumiremos $b = 0$ e eixo de simetria em $x = 0$, resultando em um mapa de um único parâmetro r, denotado de e-tanh. O gráficos deste mapa para $r = 3$ e $r = 5$ são apresentados na Fig. 1. A distribuição de pontos para

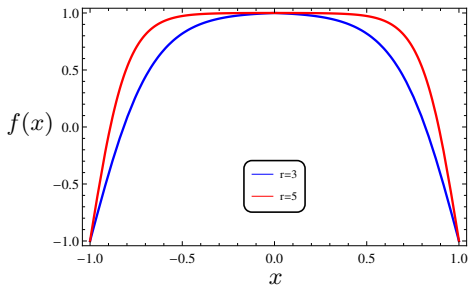

Fig. 1. O mapa e-tanh para $r = 3$ e $r = 5$.

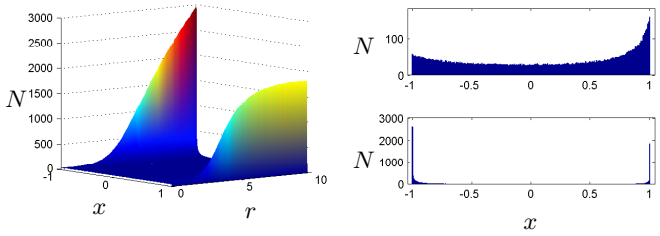

Fig. 2. Na esquerda, distribuição dos pontos de uma órbita para o mapa e-tanh com r entre 0 e 10. Na direita, o histogramas para $r = 2$ (figura superior) e $r = 9$ (figura inferior).

órbitas com 10.000 pontos para r entre 0 e 10 é apresentada à esquerda na Fig. 2. Já à direita, o histograma superior foi gerado para $r = 2$ e o inferior para $r = 9$. Observa-se que a concentração de pontos em torno de -1 e $+1$ aumenta com o valor de r, com maior tendência para -1 se $r > 7$ e para $+1$ se $r < 7$.

III. Entropia Condicional

A entropia condicional é uma medida importante para determinar a aleatoriadade de uma sequência binária [17]. Seja $\{Z_n\}_{n=1}^{\infty}$ uma sequência de variáveis aleatórias binárias estacionárias. Define-se a entropia condicional de Z_n dado os $n-1$ últimos símbolos Z^{n-1} (em que $Z^{n-1} = Z_{n-1}Z_{n-2}\cdots Z_1$) da seguinte forma [15]

$$H(Z_n \mid Z^{n-1}) = \sum_{z^n \in \{0,1\}^n} \Pr(z^n) \log_2 \left(\frac{1}{\Pr(z_n \mid z^{n-1})}\right).$$

A entropia condicional $H(Z_n \mid Z^{n-1})$ é não crescente com n para um processo estacionário e converge para a taxa de entropia H [15]

$$H = \lim_{n\to\infty} H(Z_n \mid Z^{n-1}).$$

Uma sequência aleatória ideal deve atingir $H(Z_n \mid Z^{n-1}) = 1$ para todos os valores de n. Para gerar uma sequência binária a partir do mapa e-tanh, procedemos da seguinte forma. Fixamos um valor de r e uma condição inicial x_0 e obtermos uma órbita finita usando (1). Os primeiros 400 pontos gerados são descartados devido ao transiente inicial da órbita. O intervalo $[-1, 1]$ é particionado em duas regiões $\mathcal{R}_0 = [-1, \varepsilon)$ e $\mathcal{R}_1 = [\varepsilon, 1]$ satisfazendo $\Pr(x_n \in \mathcal{R}_0) = \Pr(x_n \in \mathcal{R}_1) = 1/2$, tal que se $x_n \in \mathcal{R}_0$ então $z_n = 0$, ou se $x_n \in \mathcal{R}_1$ então $z_n = 1$.

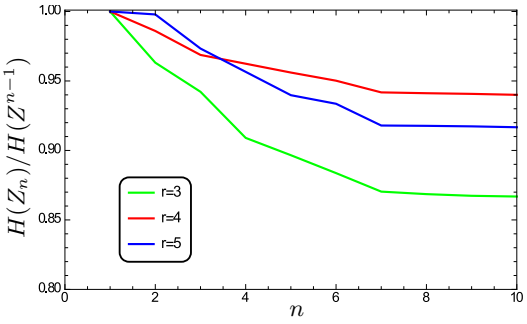

Fig. 3. $H(Z_n \mid Z^{n-1})$ versus n para mapa e-tanh para $r = 3, 4, 5$.

A Fig. 3 mostra $H(Z_n \mid Z^{n-1})$ versus n para uma sequência binária gerada por simulação para o mapa e-tanh para três valores do parâmetro r. Observa-se em todas as curvas mostradas que a entropia condicional decresce até um valor de n aproximadamente igual a 7 e após este valor converge para a taxa de entropia. Este valores são $H = 0,867$ para $r = 3$, $H = 0,94$ para $r = 4$ e $H = 0,917$ para $r = 5$. A incerteza sobre uma variável Z_n decresce com o conhecimento de valores passados até $n = 7$, o que implica a presença de uma memória finita na sequência binária. Não espera-se uma correlação relevante entre as variáveis Z_n e Z_{n+m} para $m > 7$. A próxima seção descreve o procedimento de geração de um RNG proposto neste trabalho.

IV. Geração de um RNG Baseado no Mapa e-tanh

A geração de um RNG é composta de três etapas: geração de uma órbita finita a partir de um mapa caótico, emprego da técnica de saltos de amostras [14] para reduzir a correlação da sequência caótica e, finalmente, a sequência binária é gerada usando a técnica de discretização codificada variante no tempo. O salto de amostras tem como entrada uma órbita finita gerada pelo mapa $\{x_n\}_{n=1}^{N}$ e produz na saída $\{x_{n\cdot p}\}_{n=0}^{N'}$, para um valor fixo do parâmetro p que especifica o salto de amostras. Se for aplicado o procedimento usual de mapear a sequência de saída em uma partição com duas regiões (conforme discutido na seção anterior), a sequência binária tem comprimento p vezes menor que a sequência caótica de entrada, o que compromete a taxa de bits por amostra caótica.

Para aumentar esta taxa, propomos particionar o intervalo $[-1, 1]$ em 2^q regiões, $\mathcal{R}_i$, $i = 0, \cdots 2^q - 1$, de tal forma que $\Pr(x_n \in \mathcal{R}_i) = 1/2^q$. Por exemplo, para o mapa e-tanh com $r = 3$, as quatro regiões (para $q = 2$) são [-1,-0.65), [-0.65,0.19), [0.19,0.87), [0.87,1]. Esta partição reflete a concentração do histograma em valores extremos do mapa, como mostrado na Fig. 2. Cada região é rotulada com uma sequência binária de q bits. O emprego do salto de amostras em conjunto com a discretização de 2^q regiões produz uma taxa de bits por amostra caótica, denotado de R_x, da seguinte forma:

$$R_x = q/p \tag{4}$$

Por exemplo, para $R_x = 1$ a sequência binária é a sequência caótica têm o mesmo comprimento. Por outro lado, o particionamento em duas regiões implica que $R_x = 1/p$.

O processo de codificação consiste em atribuir a cada região uma sequência de bits (denominada de sequência código). Por exemplo, uma possível codificação fixa das regiões para $q = 2$ é $(00, 01, 10, 11)$. Por exemplo, se $x_n \in \mathcal{R}_0$ então a sequência binária gerada neste intervalo é 00, se $x_n \in \mathcal{R}_1$ a sequência gerada é 01, e assim sucessivamente. O emprego de $q > 1$ propicia o surgimento de uma correlação entre os bits das sequências código de cada região, o que enfraquece a aleatoriedade da sequência binária gerada. Assim, propomos uma codificação variante no tempo (CVT) que consiste em um deslocamento cíclico para direita entre os bits que rotulam regiões adjacentes. Por exemplo, se para a n-ésima amostra caótica a codificação é $(00, 01, 10, 11)$, para a próxima amostra a codificação passa a ser $(10, 00, 11, 01)$.

A seguir, empregaremos a bateria de testes NIST para analisar a aleatoriedade de sequências binárias geradas com o procedimento proposto nesta seção. Para cada valor de r, discutiremos valores apropriados de p e q que quando associados à técnica CVT produzem RNG's com maior taxa R_x.

V. Teste de Aleatoriedade NIST

Para concluir se uma estratégia de geração um RNG é criptograficamente segura, as sequências geradas devem ser submetidas a uma variedade de testes estatísticos projetados para detectar características específicas esperadas de sequências aleatórias. Existem várias opções disponíveis de testes estatísticos, entre as quais destacamos: NIST [18], DIEHARD [19], testes de Knuth [20].

Neste trabalho empregaremos o NIST (versão 800-22) que é um pacote que compreende 15 testes estatísticos baseado em teste de hipóteses e é largamente usado na literatura. Cada teste é utilizado para determinar a aceitação ou rejeição da hipótese que detecta um desvio da aleatoriedade ideal e gera um parâmetro $P\text{-}value$ que indica a probabilidade de um gerador de números aleatórios ideal produzir uma sequência menos aleatória que a sequência testada. Este é calculado com nível de significância α, tipicamente compreendido no intervalo [0,001;0,01]. Se $P\text{-}value$ é igual a 1, então a sequência parece ter aleatoriedade perfeita, enquanto $P\text{-}value$ igual a 0 indica que a sequência parece ser completamente não-aleatória (para um dado teste). Para o valor adotado, $\alpha = 0,01$, uma sequência é aprovada com nível de significância de 99%.

Nas simulações realizadas, a sequência binária de entrada do NIST tem comprimento 524288000 (formada pela concatenação de 500 subsequências de comprimento 1048576 geradas com condições iniciais escolhidas aleatoriamente). O teste fornece como resultado o valor de $P\text{-}value$ a bem como a razão de subsequências aprovadas para cada teste da bateria NIST. A razão mínima para que a sequência passe em cada teste é calculada usando o procedimento mostrado em [18] que depende do número de subsequências e do valor de α. Para os valores considerados, esta é 0,9767. Portanto, se $P\text{-}value$ é maior que α e a razão é maior que 0,9767 então a sequência é considerada aprovada em um teste, caso contrário, a sequência é rejeitada.

A Tabela I ilustra os resultados dos testes NIST realizados para a sequência gerada pelo mapa e-tanh com $r = 3$, como

TABELA I

P-$value$ E A RAZÃO DE TESTES APROVADOS PARA CADA TESTE DO NIST, PARA O MAPA E-TANH COM $r = 3$, $R_x = 7/7$, COM CVT

Teste Estatístico	P-$value$	Aprovados	Resultado
Frequency	0.353733	0.98800	Sucesso
Block Frequency	0.041169	0.98600	Sucesso
Runs	0.911413	0.98800	Sucesso
Longest-Run-of-Ones	0.448424	0.99600	Sucesso
Binary Matrix Rank	0.021407	0.99600	Sucesso
FFT	0.197981	0.98200	Sucesso
Non-Overlapping Template	0.603841	0.99400	Sucesso
Overlapping Template	0.682823	0.99000	Sucesso
Universal	0.150340	0.99200	Sucesso
Linear Complexity	0.463512	0.98400	Sucesso
Serial	0.649612	0.98800	Sucesso
Approximate Entropy	0.073201	0.98800	Sucesso
Random Excursions	0.023545	0.98214	Sucesso
Random Excursions Variant	0.122325	0.98276	Sucesso
Cumulative Sums	0.767582	0.99600	Sucesso

TABELA II

MAIORES TAXAS R_x ALCANÇADAS COM CODIFICAÇÃO FIXA E CVT, PARA O MAPA E-TANH COM $r = 3, 4, 5$

Salto	$r = 3$		$r = 4$		$r = 5$	
	CVT	Fixa	CVT	Fixa	CVT	Fixa
$p = 6$	5/6	X	5/6	X	4/6	X
$p = 7$	7/7	1/7	7/7	X	5/7	X
$p = 8$	–	2/8	–	1/8	–	X
$p = 9$	–	3/9	–	–	–	1/9

parâmetros $p = 7$, $q = 7$, $R_x = 7/7$, com CVT. Este gerador passa em todos os testes realizados, portanto é um RNG de alta qualidade de acordo com o teste NIST. Convém ressaltar que a taxa de entropia para esta sequência é $H = 0,9999$ o que é um indicador adicional da aleatoriedade da sequência binária gerada.

A Tabela II apresenta as maiores taxas R_x alcançadas, com codificação fixa e CVT, que passaram no teste NIST para cada valor do salto p para o mapa e-tanh para três valores de r. Nesta tabela, o símbolo X indica que o gerador não passa no teste para os parâmetros indicados, enquanto o símbolo "–" indica que não é possível aumentar a taxa em relação à mostrada na mesma coluna para um valor menor de p. O emprego de CVT permite aumentar substancialmente a taxa, como é observado na tabela para $r = 3$ e $p = 7$, em que $R_x = 1/7$ é obtida com a codificação fixa e $R_x = 7/7$ com a CVT. O gerador não passa no teste para $p = 7$ e codificação fixa para $r = 4$ e $r = 5$. O aumento do salto para $p = 8$ ou $p = 9$ ainda permite obter um bom gerador com codificação fixa para $q > 1$, embora com taxa baixa. Observa-se que é possível obter um gerador com taxa menor que 1 que passe nos testes com $p = 6$ e CVT. O esquema CVT atinge a maior taxa (unitária) com $p = 7$ para todos os valores de r.

Convém ressaltar que $p = 7$ é o valor do salto indicado pela entropia condicional mostrada na Fig. 3 para a quebra da correlação da sequência binária gerada com $q = 1$. Portanto, a informação gerada pela entropia condicional é importante para a determinação do valor do salto de amostras p.

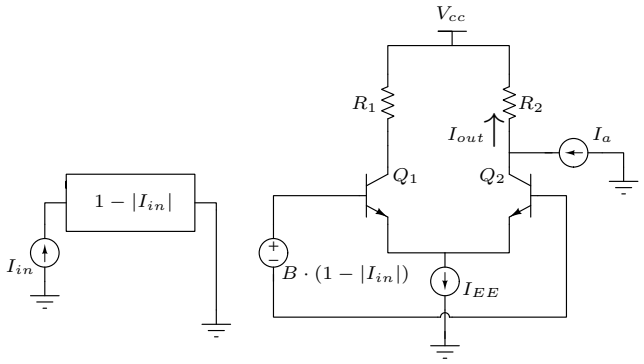

Fig. 4. Circuito para implementação do mapa e-tanh.

VI. IMPLEMENTAÇÃO DO E-TANH

O mapa e-tanh é reescrito a partir de (2) da seguinte forma:

$$f(x) = e \cdot \tanh\big[r \cdot (1 - |x|)\big] - 1. \tag{5}$$

Para implementação deste mapa, emprega-se o circuito da Fig. 4, que é baseado em um par diferencial com transistor bipolar de junção (TBJ). Denominamos por $v_{id} = B(1-|I_{in}|)$ a tensão diferencial entre os terminais base de Q_1 e Q_2, I_{EE} a corrente de polarização do par diferencial e V_T a tensão térmica, uma constante em torno de $26mV$. A entrada do circuito é I_{in} e a saída é o inverso da corrente de coletor de Q_2 mais uma corrente constante I_a, ou seja, $I_{out} = -I_2 + I_a$. Pode-se mostrar que I_2 é função da tangente hiperbólica da tensão diferencial por um fator de escala $2 \cdot V_T$ [21], o que permite especificar I_{out} da seguinte forma

$$I_{out} = \frac{I_{EE}}{2} \cdot \tanh\left(\frac{v_{id}}{2 \cdot V_T}\right) - \left(\frac{I_{EE}}{2} - I_a\right). \tag{6}$$

Para especificar (5) em termos dos parâmetros do circuito, a corrente I_{out} deve ser normalizada. Aplicando esse fator de normalização para toda a equação, a transresistência B é escolhida para gerar o respectivo argumento da tangente hiperbólica em (5) e a corrente I_a é escolhida para que o segundo termo do lado direito da equação (6) seja igual a unidade quando normalizado.

Com o auxílio de um circuitos periféricos apropriado é possível gerar uma sequência do mapa e-tanh. Entre esses periféricos, destaca-se o papel do circuito *sample-and-hold* [22], que permite gerar uma sequência caótica a partir do núcleo apresentado na Fig. 4. Isso ocorre com a amostragem de I_{out} em um ciclo de máquina (sample) e o emprego deste como entrada no ciclo subsequente. Para gerar a próxima saída do mapa é preciso aguardar a estabilização da saída após a atualização da entrada (hold). Este processo permite implementar eletronicamente o mecanismo de "iteração" do mapa descrito em (1).

Para validar o circuito proposto são realizadas simulações com o software NGSPICE. Para ilustrar o seu funcionamento o parâmetro r é fixado em $r = 5$. O modelo padrão para transistor TBJ do NGSPICE é usado na simulação. Os resistores R_1 e R_2 são escolhidos de forma que os transistores sempre operem na região ativa, no nosso caso $R_1 = R_2 = 100\,\Omega$. A Fig. 5 compara a curva característica do circuito com a obtida pelo mapa em (5), observando-se uma sobreposição

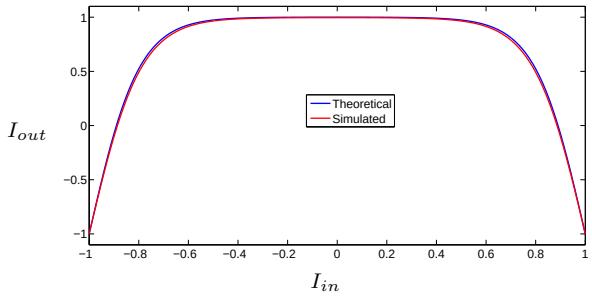

Fig. 5. Comparação entre a curva teórica e a curva característica do circuito para $r = 5$.

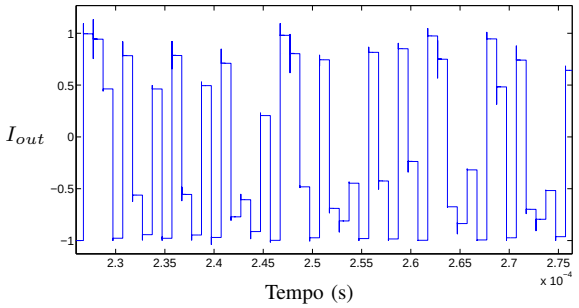

Fig. 6. Resposta no tempo do circuito para $r = 5$.

destas curvas. A Fig. 6 mostra uma realização da sequência temporal da corrente de saída o circuito, em que observa-se seu comportamento errático.

VII. Conclusões

Apresentamos uma nova metodologia para o projeto de RNG's que considera a otimização da taxa de bits por amostra caótica. Mostramos como a entropia condicional pode ser empregada para especificar o salto de amostras, além disso, propusemos um processo de codificação das amostras que não degrada a taxa de geração de bits, como comumente ocorre com outras propostas. Empregando o teste NIST concluímos que a sequência obtida pela metodologia proposta apresenta boas propriedades criptográficas. Por fim, mostramos a viabilidade prática da proposta com a apresentação de um circuito que implementa o mapa considerado neste trabalho.

Referências

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

[2] K. Alligood, T. Sauer, and J. Yorke, *Chaos: An Introduction to Dynamical Systems*. New York, NY, 1997.

[3] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, pp. 3031–3034, May 1993.

[4] J. Chen, J. Zhou, and K.-W. Wong, "A modified chaos-based joint compression and encryption scheme," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 58, pp. 110–114, Feb 2011.

[5] A. Masmoudi and W. Puech, "Lossless chaos-based crypto-compression scheme for image protection," *IET Image Processing*, vol. 8, no. 12, pp. 671–686, 2014.

[6] F. Lau and C. Tse, *Chaos-Based Digital Communication Systems*. Engineering online library, Springer, 2010.

[7] M. Eisencraft, R. Attux, and R. Suyama, *Chaotic Signals in Digital Communications*. Electrical Engineering & Applied Signal Processing Series, Taylor & Francis, 2013.

[8] P. Stavroulakis, *Chaos Applications in Telecommunications*. Taylor & Francis, 2005.

[9] L. Kocarev and S. Lian, *Chaos-based Cryptography: Theory, Algorithms and Applications*. Studies in Computational Intelligence, Springer, 2011.

[10] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, pp. 1498–1509, Dec. 2001.

[11] L. Kocarev, J. Makraduli, and P. Amato, "Public-key encryption based on chebyshev polynomials," *Circuits, Systems and Signal Processing*, vol. 24, no. 5, pp. 497–517, 2005.

[12] T. Stojanovski and L. Kocarev, "Chaos-based random number generators-part I: analysis [cryptography]," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 48, pp. 281–288, Mar 2001.

[13] L. De Micco, H. A. Larrondo, A. Plastino, and O. A. Rosso, "Quantifiers for randomness of chaotic pseudo-random number generators," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 367, no. 1901, pp. 3281–3296, 2009.

[14] L. D. Micco, C. González, H. Larrondo, M. Martin, A. Plastino, and O. Rosso, "Randomizing nonlinear maps via symbolic dynamics," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 14, pp. 3373 – 3383, 2008.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 2006.

[16] D. Chaves, C. Souza, and C. Pimentel, "A new map for chaotic communication," in *Telecommunications Symposium (ITS), 2014 International*, pp. 1–5, Aug 2014.

[17] A. Beirami and H. Nejati, "A framework for investigating the performance of chaotic-map truly random number generators," *IEEE Transactions on ciucuits and systems -II: Express Briefs*, vol. 60, no. 7, pp. 446 – 450, 2013.

[18] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "Statistical test suite for random and pseudo random number generators for cryptographic applications.," *Special Publication 800-22 Revision 1a, National Institute of Standards and Technology*, April 2010.

[19] G. Marsaglia, "Diehard statistical tests," 1995.

[20] D. Knuth, *The Art of Computer Programming: Seminumerical algorithms*. Addison-Wesley series in computer science and information processing, Addison-Wesley, 1981.

[21] D. Pederson and K. Mayaram, *Analog Integrated Circuits for Communication: Principles, Simulation, and Design*. Kluwer Academic Publishers, 1991.

[22] P. Dudek and V. Juncu, "Compact discrete-time chaos generator circuit," *Electronics Letters*, vol. 39, pp. 1431–1432, Oct 2003.