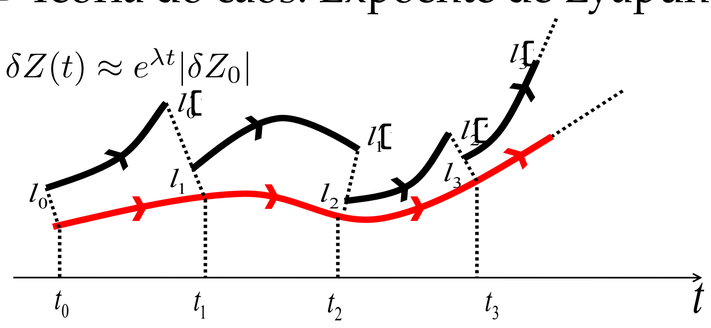
Expoente de Lyapunov: Classificação qualitativa dos modos de operação na criptografia

Machicao, Jeaneth; Anderson Marco; Bruno, Odemir
Grupo de Física Interdisciplinar, Instituto de Física de São Carlos, USP
machicao@ursa.ifsc.usp.br/ bruno@ifsc.usp.br

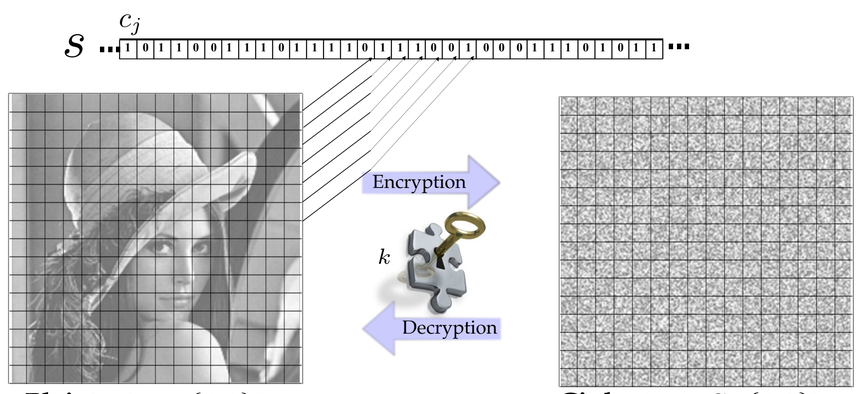
Teoria do caos: Expoente de Lyapunov

$$\delta Z(t) \approx e^{\lambda t}|\delta Z_0|$$



$$\lambda(t) = \lim_{t\to\infty} \frac{1}{t} \log \left| \frac{\delta Z_t}{\delta Z_0} \right|$$

Criptografia: Cifradores de Bloco



Plaintext $P : \{0,1\}^n$ **Ciphertext** $C : \{0,1\}^n$

$$E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

Modos de operação

Modos de operação do NIST	Modos de operação isolados M
• Electronic Codebook	M_{ECB} : $C_i = P_i$
• Cipher Block Chaining	M_{CBC} : $C_i = C_{i-1} \oplus P_i$, $C_0 = IV$
• Output Feedback	M_{OFB} : $C_i = P_i \oplus O_i$, $O_i = O_{i-1}$, $O_1 = IV$
• Cipher Feedback	M_{CFB} : $C_i = P_i \oplus C_{i-1}$, $C_1 = P_1 \oplus IV$
• Counter mode	M_{CTR} : $C_i = P_i \oplus O_i$, $P_i = C_i \oplus O_i$, $O_i = ctr_i$, $ctr_i = rand(ctr_{i-1})$, $ctr_1 = rand(IV)$

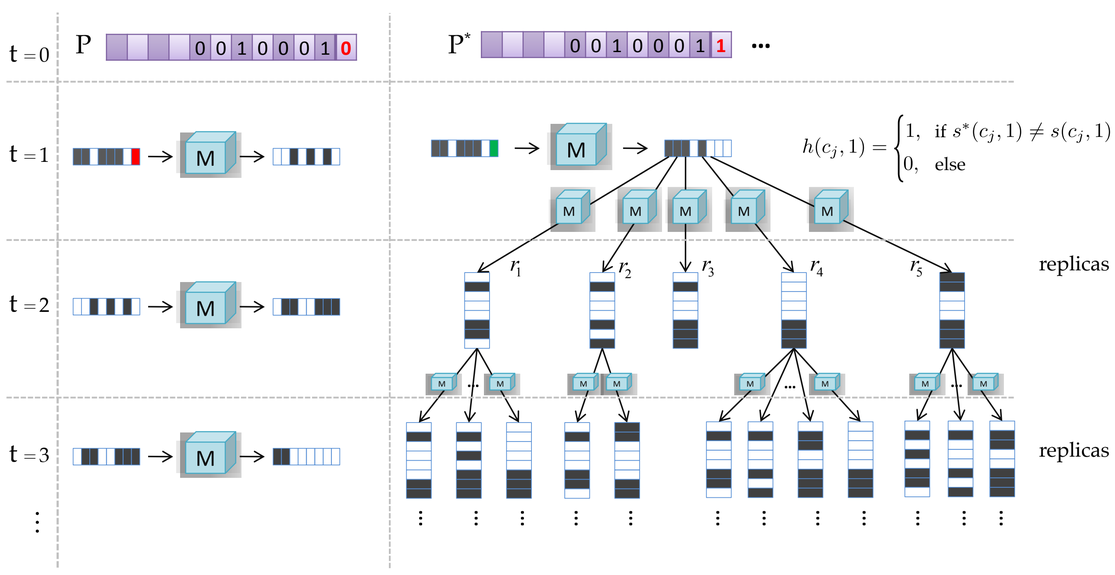
$$M_{mode} : \{0,1\}^n \to \{0,1\}^n$$

Sistemas Dinâmicos — $\lambda(t) = ?$ — $s(\cdot, t+1) = M(s(\cdot, t))$ — $\langle C, s, P, M \rangle$ — Autômatos Celulares

Resumo

Muitos pesquisadores evidenciaram a relação entre a teoria do caos e a criptografia [1-2]. Pouca atenção foi dada para uma das perguntas mais desafiadoras na criptografia: **Como comparar qualitativamente entre os modos de operação de cifradores de blocos?** Para superar essa falta propomos uma metodologia através de algumas analogias com sistemas dinâmicos discretos. O método consiste na medida de caos dos modos de operação por cálculos do expoente de Lyapunov (LE). Optamos por explorar as curvas resultantes do LE para comparar entre os 5 modos do NIST [3]: ECB, CBC, OFB, CFB e CTR.

Algoritmo proposto para calcular o LE [4]



$$\lambda(t) = \frac{1}{t} \log \left(\frac{\sum_{r^j} \sum_{c_i} h(c_i, t)}{\sum_{c_i} h(c_i, 0)} \right)$$

Resultados: Classificação dos modos de operação

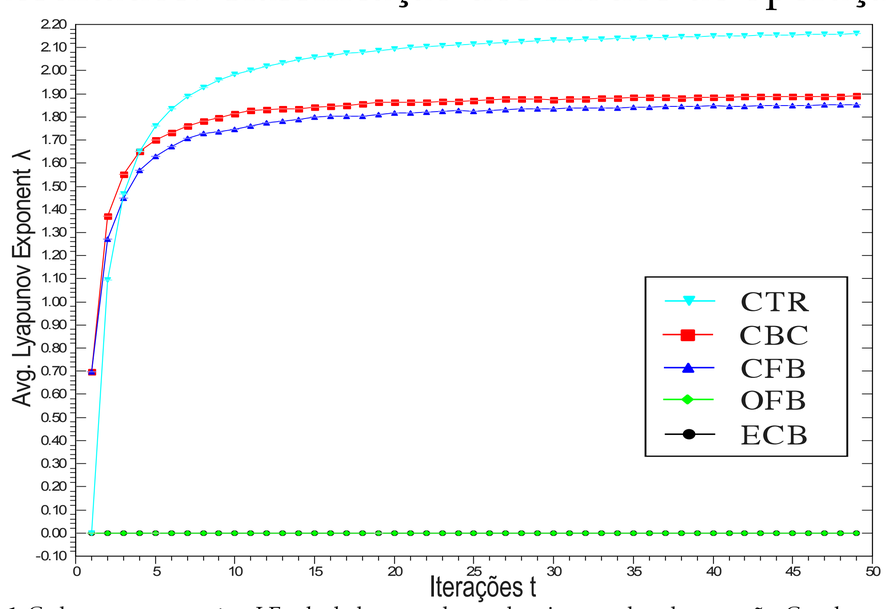


Fig. 1. Cada curva representa o LE calculado por cada um dos cinco modos de operação. Com base na posição colocada das curvas de cima para baixo, a lista de classificação em ordem de qualidade é: CTR, CBC, CFB, OFB e ECB (em ordem decrescente) para os modos de operação do NIST. Além disso, estes resultados podem ser contrastados visualmente com um análise posterior.

Análise visual do espectro de potencia do Fourier

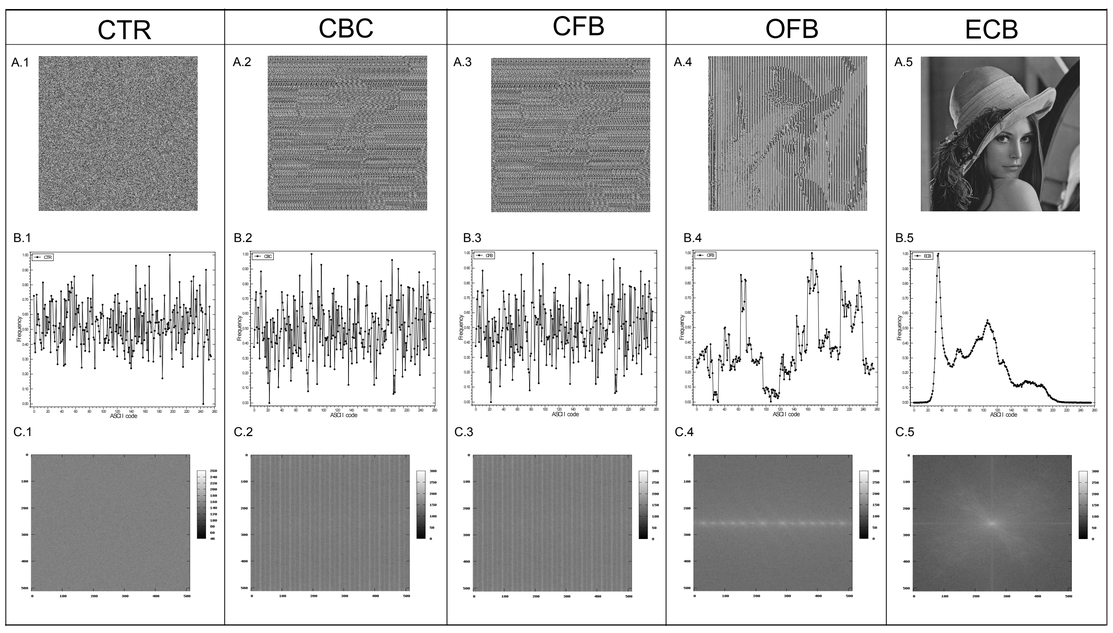


Fig 2. Comparação dos cinco modos de operação: (A) imagem de entrada, (B) Histograma e (C) Espectro de potência de Fourier (Power spectrum Fourier), da esquerda para a direita, nessa ordem é: CTR, CBC, CFB, OFB e ECB.

Conclusões

- Corroboramos a forte relação entre a teoria do caos ea criptografia.
- O expoente de Lyapunov aplicada aos modos de operação do NIST podem classificá-las qualitativamente.
- Isto representa um grande avanço na criptografia desde que os usuários possam conhecer a qualidade do cifrado.

Referências

[1] J. Amigó, J. Szczepanski, and L. Kocarev, "Discrete chaos and cryptography," *International Symposium on Nonlinear Theory and its Applications (NOLTA2005)*, pp. 461-464, 2005.

[2] G. Millerioux, J. M. Amigó, and J. Daafouz, "A connection between chaotic and conventional cryptography," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 55, no. 6, pp. 1695-1703, 2008.

[3] M. Dworkin, "Recommendation for block cipher modes of operation," tech. rep.,*National Institute of Standards and Technology*, 2001.

[4] J. Machicao, J. M. Baetens, A. Marco, B. De Baets, and O. Bruno, "Towards a spectral discrimination of cryptography mode of operation." [to-appearing], 2012.

Agradecimentos FAPESP