Trabalho apresentado no XLI CNMAC, Unicamp - Campinas - SP, 2022.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Sistema de criptografia de chave pública baseado em sistemas de funções fractais (IFS)

Allan H. Tanaka[1]
UNESP, Bauru, SP
Tatiana M. Rodrigues[2]
UNESP, Bauru, SP

Este estudo tem como objetivo a análise de aspectos matemáticos das funções fractais e sua aplicação na criptografia, em específico os sistemas de criptografia de chaves públicas, levando em consideração a eficiência e a segurança do método.

Conforme [2], em sistemas de criptografia de chave pública é utilizado um par de chaves assimétricas, através de um algoritmo c para criptografar e d para descriptografar, cada usuário tem um par de chaves (C_k, D_k) tal que para uma mensagem m, exista a identidade $d(c(m, C_k), D_k) = m$, onde a chave D_k é privada, que é utilizada para descriptografar a mensagem que foi criptografada pela chave C_k, que pode ser publicada a quem desejar ter acesso.

De acordo com [3] e [1], desde o ano de 1990, muitos pesquisadores notaram que existe uma relação muito interessante entre caos, a geometria fractal e a criptografia. Os sistemas dinâmicos caóticos têm por característica serem muito sensíveis a condições iniciais, terem uma geometria muito complexa, além de um comportamento aleatório. Em particular, funções fractais possuem uma estrutura matemática complicada, especialmente na construção recursiva de tais funções, fornecendo melhores aproximações, as quais geram alguns aspectos muito úteis na área de criptografia.

A teoria fractal pode ser definida através de sistemas de funções iteradas, de modo que tais conjuntos de equações representam rotação, translação e escala, gerando uma imagem fractal, para isto, algumas definições são necessárias, ainda baseado em [3] e [1].

Definição 0.1. *Consideremos um espaço métrico (X, d), o espaço de todos os subconjuntos compactos não-vazios de X é chamado de Espaço de Hausdorff denotado por $\mathcal{H}(X)$, com isto, é possível definir a distância h de Hausdorff em $\mathcal{H}(X)$, considerando A, B subconjuntos de X, temos:*

$$h(A, B) = max\{inf\{\varepsilon > 0; B \in (A - \varepsilon, A + \varepsilon)\},\ inf\{\varepsilon > 0; A \in (B - \varepsilon, B + \varepsilon)\}\}. \tag{1}$$

Definição 0.2. *Tomemos dois espaços métricos (X, d_X) e (Y, d_Y), a transformação $T : X \to Y$ é dita ser uma contração se, e somente se, existe $s \in \mathbb{R}$, $0 < s < 1$, tal que $d_Y(T(x_i), T(x_j)) \leq s \cdot d_X(x_i, x_j)\ \forall x_i, x_j \in X$, onde s é o fator de contração de T.*

Teorema 0.1. *Seja uma contração $T : X \to X$ em um espaço métrico completo (X, d). Logo, existe um único ponto x_f tal que $T(x_f) = x_f$. Além disso, para todo $x \in X$, temos que $\lim_{n\to\infty} T^{o_n}(x) = x_f$, onde T^{o_n} denota a n-ésima composição de T.*

Com isto, pode-se dizer que um fractal é construído a partir de cópias de transformações de si mesmo, sendo tais transformações realizadas por um conjunto de transformações afins $G : \mathbb{R}^2 \to \mathbb{R}^2$ da forma

[1] allan.tanaka@unesp.br
[2] tatiana.rodrigues@unesp.br

$$\begin{pmatrix} u \\ v \end{pmatrix} = G \begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} = A \cdot X + b, \tag{2}$$

onde (u, v) e $(x, y) \in \mathbb{R}^2$.

De acordo com as Definições (0.1) e (0.2), podemos definir a transformação $K : G(X) \to G(X)$, conhecida como o operador de Hutchinson,

$$A = K(B) = \bigcup_{i=1}^{N} T(B). \tag{3}$$

Desta forma, o método de criptografia proposto é baseado na escolha de um fractal conhecido, a partir das soluções de suas transformações afins dadas recursivamente, com números de iterações definidos pelo atrator do fractal, o qual é gerado através do operador de Hutchinson.

O algoritmo fractal é capaz de suportar ataques à segurança do sistema com eficácia, pois é demasiadamente demorado solucionar sistemas não-lineares numericamente, os erros de aproximação e truncamento durante o processo de solução ocasionam a mudança da ordem das transformações afins, gerando assim uma mudança drástica na imagem do fractal.

Levando em conta tais considerações, a ameaça de ataques será pequena, pois mesmo o invasor conseguindo acesso a alguns componentes da chave, ao cometer um leve erro de aproximação, a aleatoriedade do fractal o levará em valores inviáveis.

Referências

[1] M. F. Barnsley. **Fractals Everywhere**. 1a. ed. Atlanta, Georgia: Academic Press, 1988. ISBN: 0-12-079062-9.

[2] R. C. Miritz. "Criptografia de chave pública". Dissertação de mestrado. Universidade Federal do Rio Grande do Sul, 2000.

[3] N. M. G. AL-Saidi, M. R. Md. Said e A. M. Ahmed. "Efficiency Analysis for Public Key Systems Based on Fractal Functions". Em: **Journal of Computer Science** 7 (2011), pp. 526–532.