Efficiency and Robustness of a Hyperchaos Based Cryptography Scheme

Fabiano Alan Serafim Ferrari[1,2], Walber Franklin Rodrigues Pinheiro[2]

[1] Technological University of Parana, Department of Physics, Pato Branco, Brazil,
[2] State University of Montes Claros, Graduate Program in Computational Modelling and Systems, Montes Claros, Brazil,

The world dependence on internet and technology has made cryptography a serious issue in current society, whitout it our banks accounts, personal data and privacy would certain be in jeopardy. At the same time, the technological development, the expansion of artificial intelligence, quantum computation, and other scientific advances require constant evolution and adaptation of the standard cryptography algorithms. While the standard methods are based on prime numbers factorization and permutation schemes, we focus on the use of pseudorandom properties of chaotic attractors. The most used cryptography algorithms are: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Blowfish and Twofish [1]. Among the most popular chaos based cryptography is the Baptista's method, where a piecewise linear map is used [2]. Currently, many chaos based cryptography methods have been proposed, and they can be as secure as the standard methods [3]. One of the main issues in chaos based cryptography is the efficiency, usually the system requires a significant transient time to avoid potential biases and correlations. To overcome this problem, we propose the use of a high dimension hyperchaotic system. We also tested our system against the traditional types of attacks, such as "Known-Plaintext Attack" and "Brutal Force Attack". Our results shows that hyperchaotic system perform better than chaotic maps, are more robust, and the use of permutation between variables in high dimension maps can make chaos based cryptography efficient. We thanks Fundação Araucária and UTFPR for financial support.

References

[1] HAMZA, Aljaafari; KUMAR, Basant. A review paper on DES, AES, RSA encryption standards. In: 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART). IEEE, 2020. p. 333-338.

[2] BAPTISTA, M. S. Cryptography with chaos. Physics letters A, 1998, 240.1-2: 50-54.

[3] ALVAREZ, Gonzalo; LI, Shujun. Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 2006, 16.08: 2129-2151.

Type

ORAL