Efficiency analysis for public key systems based on fractal functions.

ABSTRACT

In the last decade, dynamical systems were utilized to develop cryptosystems, which ushered the era of continuous value cryptography that transformed the practical region from finite field to real numbers. Approach: Taking the security threats and privacy issues into consideration, fractals functions were incorporated into public-key cryptosystem due to their complicated mathematical structure and deterministic nature that meet the cryptographic requirements. In this study we propose a new public key cryptosystem based on Iterated Function Systems (IFS). Results: In the proposed protocol, the attractor of the IFS is used to obtain public key from private one, which is then used with the attractor again to encrypt and decrypt the messages. By exchanging the generated public keys using one of the well known key exchange protocols, both parties can calculate a unique shared key. This is used as a number of iteration to generate the fractal attractor and mask the Hutchinson operator, so that, the known attacks will not work anymore. The algorithm is implemented and compared to the classical one, to verify its efficiency and security. We conclude that public key systems based on IFS transformation perform more efficiently than RSA cryptosystems in terms of key size and key space.

Keyword: Public key system; Fractal fractions; Attractor.