A new public key cryptosystem based on IFS

ABSTRACT

Most public key encryption methods suffers from the inability to prove the difficulty of the algorithms, which summarizes under the category of mathematical problems that have inverses which are believed (but not proven) to be hard. The length and strength of the Cryptography keys are considered an important mechanism. The keys used for encryption and decryption must be strong enough to produce strong encryption. Fractals and chaotic systems have properties which have been extensively studied over the years, and derive their inherent complexity from the extreme sensitivity of the system to the initial conditions. In this paper a new cryptographic system based on Iterated Function Systems (IFS) have been proposed to reduce the computation cost and increase the security for the public-key cryptography protocols. In the proposed public-key encryption algorithm, generate iterated function systems as a global public element, then its Hutchinson operator is used as a public key. To encrypt the plaintext with the receiver's public key we use one of the key agreement protocols to generate a shared private key that used to find the attractor of the IFS. The chaotic nature of the fractal functions ensures the security of the proposed public-key cryptosystem schemes

Keyword: Public key cryptosystem; Public key encryption method; Fractal; Chaotic system