American Journal of Applied Sciences x (x): xx-xx, 2007

ISSN 1546-9239

' 2007 Science Publications

**A New Digital Signature Scheme Based on Mandelbrot and Julia Fractal Sets**

Mohammad Ahmad Alia and Azman Bin Samsudin,

School of Computer Sciences Universiti Sains Malaysia (USM) 11800 Penang, Malaysia.

**Abstract:** This paper describes a new cryptographic digital signature scheme based on Mandelbrot and Julia fractal sets. Having fractal based digital signature scheme is possible due to the strong connection between the Mandelbrot and Julia fractal sets. The link between the two fractal sets is used for the conversion of the private key to the public key. Mandelbrot fractal function takes the chosen private key as the input parameter and generates the corresponding public-key. Julia fractal function is then used to sign the message with receiver’s public key and verify the received message based on the receiver’s private key. The propose scheme is resistant against attacks, utilizes small key size and performs comparatively faster than the existing DSA, RSA digital signature scheme. Therefore, the fractal digital signature scheme is an attractive alternative to the traditional number theory digital signature scheme.

**Keywords:** Fractals Cryptography, Digital Signature Scheme, Mandelbrot Fractal Set, and Julia Fractal Set.

# **INTRODUCTION**

Cryptography is the science of information security. Cryptographic system in turn, is grouped according to the type of the key system: symmetric (secret-key) algorithms which utilizes the same key (see Fig. 1) for both encryption and decryption process, and asymmetric (public-key) algorithms which uses different, but mathematically connected, keys for encryption and decryption (see Fig. 2). In general, cryptography protocol employs public-key algorithm to exchange the secret key and then uses faster symmetric algorithms to ensure secrecy of the data stream [1, 2].

Public-key scheme is based on the idea that a user can possess two keys, one key is known to the public and the other is private to the owner. The public-key algorithm uses the public key to encrypt the data to be sent, and then at the recipient side, uses the private key to decrypt the ciphered data. Digital signature is a verification mechanism based on the public-key scheme that is focusing on message authenticity. The output of the signature process is called the digital signature [2].