IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7

# Generalized Scheme For Fractal Based Digital Signature (GFDS)

**Mohammad Ahmad Alia and Azman Bin Samsudin*,*** *mohahmadalia.cod05@student.usm.my, azman@cs.usm.my*

School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia.

## Summary

This paper describes a new development in the cryptographic digital signature scheme based on Mandelbrot and Julia fractal sets. Recently it has been shown that it is possible to have digital signature scheme based on fractal 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 a public key. However in the previous work the verification can be done only by a specific party. In this paper we introduce a new variation of the fractal publickey digital scheme (GFDS), whereby the verification of the digital signature can be done by any member of the public.

***Key words:***

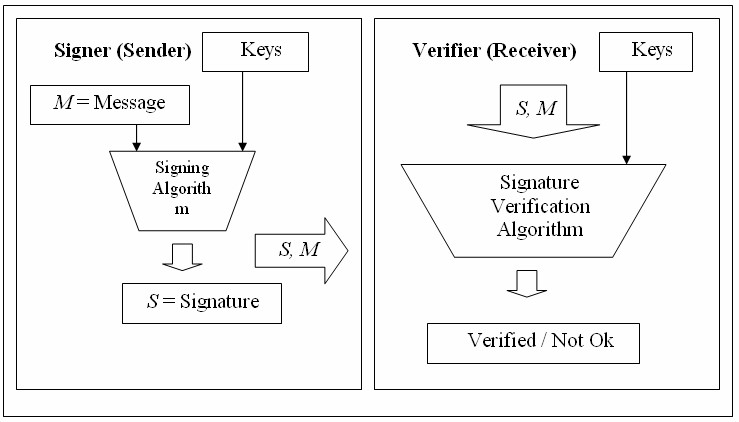
Fractals Cryptography, Digital Signature Scheme,

Mandelbrot Fractal Set, and Julia Fractal Set.

## 1. Introduction

Digital signature is an electronic verification mechanism based on the public-key scheme and is considered as a type of the asymmetric cryptography that is focusing on message authenticity. The digital signature scheme is used to provide a guarantee that the original content of a message is unchanged by unauthorized party which is known as the data integrity, the assurance that the source of data is as claimed which is known as message authentication, and the assurance that an entity cannot deny commitments which is known as non-repudiation [1, 2]. The output of the signature process is called the digital signature [3] (see Figure 1). In digital signature based on public-key algorithms, the private key is used to sign a message, while the public key is used to verify the authenticity of the message.

In 1976, Whitfield Diffie and Martin Hellman gave the first notion of a digital signature scheme although at that time they only conjectured the existence of such scheme [4, 5]. Soon after that, in 1978 Rivest, Shamir, and Adleman proposed the first digital signature scheme that is called RSA digital signature algorithm [6]. Subsequently, few more proposed digital signature algorithms based on different ‘hard problems’ were soon developed after RSA, such as ElGamal signature scheme [7], Undeniable signature [8] and others.

 Figure 1: Digital signature scheme.

The well known digital signature schemes can be classified according to the inherited mathematical problems. As of now, there are three main different NPhard problems (Non-Deterministic Polynomial) where well-known digital signature schemes have been derived from.

1. Integer Factorization (IF) schemes. The security in integer factorization schemes are based on the complexity of the integer factorization problem. Examples of IF scheme implementation are RSA digital signature scheme [6] and Rabin digital signature scheme [9].

1. Discrete Logarithm (DL) schemes. Discrete logarithm schemes are based on the complexity of the discrete logarithm problem in a specific finite field. Examples