IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.2, February 2007

**New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets**

Mohammad Ahmad Alia and Azman Bin Samsudin,

*School of Computer Sciences, Universiti Sains Malaysia.*

# Summary

In this paper, we propose a new cryptographic key exchange protocol based on Mandelbrot and Julia Fractal sets. The Fractal based key exchange protocol is possible because of the intrinsic connection between the Mandelbrot and Julia Fractal sets. In the proposed protocol, 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 calculate the shared key based on the existing private key and the received public key. The proposed protocol is designed to be resistant against attacks, utilizes small key size and comparatively performs faster then the existing Diffie-Hellman key exchange protocol. The proposed Fractal key exchange protocol is therefore an attractive alternative to traditional number theory based key exchange protocols.

***Key words:***

*Fractals Cryptography, Key- exchange protocol, Mandelbrot Fractal set, and Julia Fractal set.*

# 1. Introduction

Cryptography algorithms are classified into two categories, secret key (symmetric) algorithms and public key (asymmetric) algorithms. In general, cryptography protocol employs public key cryptosystem to exchange the secret key and then uses faster secret key algorithms to ensure confidentiality of the data stream [1, 2]. Secret key algorithm is used to encrypt and decrypt messages by using the same secret key. Public key algorithm on the other hand, works in a very different way. In public key encryption algorithm, there are two keys, both belong to the recipient. One key is known to the public, and is used to encrypt information that need to be send to the receiver who owns the corresponding private key.

The Diffie-Hellman (DH) algorithm was the first key exchange algorithm to utilize public-key concept to exchange the shared key. Public key based key exchange protocol rises above the difficulties faces by the secret key cryptosystem. This is because key management is much easier with the help of a key exchange protocol such as DH. In a secret key algorithm, both parties shared the same secret key. However the process of sharing the secret key between both the sender and the recipient, introduces a new set of problem – key distribution problem. Public key cryptosystem alleviates the key distribution problem by using two keys, a private and a public key. In most cases, by exchanging the public keys, both parties can calculate a unique shared key, known only to both of them [2, 3, 4].

This paper proposed a new Fractal (Mandelbrot and Julia Fractal sets) key exchange protocol as a method to securely agree on a shared key. The proposed method achieved the secure exchange protocol by creating a shared secret through the use of the Mandelbrot and Julia Fractal sets.

## 2.1. Fractals

A complex number consists of a real and an imaginary component. It is common to refer to a complex number as a "point" on the complex plane. If the complex number is *Z = (a + bi)*, the coordinate of the point is, *a* for the horizontal real axis, and *b* for the vertical imaginary axis.

The unit of imaginary numbers is defined as [5].

Fractals on the other hand are fragmental geometric shape that is created interactively from almost similar smaller components [6]. From another perspective, Fractals are an example of a Chaos system, where by changing the initial parameters to the system, even slightly, can generate a totally new Fractal image altogether [7]. Figure 1 shows two examples of Fractal sets, Mandelbrot Fractal set and Julia Fractal set.

 (a) (b) Figure 1: Mandelbrot and Julia Fractal sets; (a) Mandelbrot image, (b) Julia image [4].