Journal of Computer Science 4 (5): 408-414, 2008

ISSN 1549-3636

© 2008 Science Publications

# Fractal (Mandelbrot and Julia) Zero-Knowledge Proof of Identity

Mohammad Ahmad Alia and Azman Bin Samsudin

School of Computer Sciences, University Sains Malaysia, 11800 Penang, Malaysia

**Abstract:** We proposed a new zero-knowledge proof of identity protocol based on Mandelbrot and Julia Fractal sets. The Fractal based zero-knowledge protocol was possible because of the intrinsic connection between the Mandelbrot and Julia Fractal sets. In the proposed protocol, the private key was used as an input parameter for Mandelbrot Fractal function to generate the corresponding public key. Julia Fractal function was then used to calculate the verified value based on the existing private key and the received public key. The proposed protocol was designed to be resistant against attacks. Fractal based zero-knowledge protocol was an attractive alternative to the traditional number theory zero-knowledge protocol.

**Key words:** Zero-knowledge, cryptography, fractal, mandelbrot fractal set and julia fractal set .