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

Mohammad A. Alia and Azman B. Samsudin

**DOI :**10.3844/jcssp.2008.408.414

*Journal of Computer Science*

Volume 4, Issue 5

Pages 408-414

**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.