A new idea in zero knowledge protocols based on iterated function systems

ABSTRACT

A secure method of identification is crucial to avoid computer deception dynamics. This could be attained by using zero-knowledge protocols. Zero-knowledge protocols are cryptographic protocols that have been proven to provide secure entity authentication without revealing any knowledge to any entity or to any eavesdropper and used to build effective communication tools and ensure their privacy. Many schemes have been proposed since 1984. Among them are those that rely on factoring and discrete log which are practical schemes based on NP- hard problems. Our aim is to provide techniques and tools which may be useful towards developing those systems. Fractal code was proven as a NP-hard problem, which means it cannot be solved in a practical amount of time. In this paper a new zero-knowledge scheme is proposed based on iterated function systems and the fractal features are used to improve this system. The proposed scheme is a generalization of the Guillou-Quisquater identification scheme. The two schemes are implemented and compared to prove their efficiency and security. From the implementation results, we conclude that zero knowledge systems based on IFS transformation perform more efficiently than GQ system in terms of key size and key space.

Keyword: Zero-knowledge; Fractal; Iterated function systems (IFS); Guillou-Quisquater protocol; Attractor