On the security of digital signature protocol based on iterated function systems.

ABSTRACT

A common goal of cryptographic research is to design protocols that provide a confidential and authenticated transmission channel for messages over an insecure network. Hash functions are used within digital signature schemes to provide data integrity for cryptographic applications. In this paper, we take a closer look at the security and efficiency of the digital signature protocol based on fractal maps. This new system can be expected to have at least the same computational security against some known attacks. A Diffie-Hellman algorithm is used to improve the security of the proposed protocol by generating the number of iteration that is used to find the attractor of the iterated function system, which is used to calculate the public key and the signature. The proposed algorithm possesses sufficient security against some known attacks applicable on finite field cryptosystems. They are considered as time consuming to be involved in solving non-linear systems numerically over the defined infinite subfield.

Keyword: Digital signature; Fractal maps; Iterated function systems.