The Hash Algorithm Based on Three-Body Chaotic Motion

Zhang, Huayi (School: Shanghai Kongjiang Senior High School)

Hash algorithm is an algorithm that scrambles and mixes any set of input data, and outputs a highly irregular fixed length summary, it's often used in the field of information security. The author thinks of the novel "three bodies", in which the chaotic motion of the three bodies also has the characteristics of irregularity .Three body chaotic motion refers to the irregular motion of three particles whose mass, initial position and initial velocity are arbitrary under the action of mutual gravitation. Inspired by it, the author conceives a hash algorithm TB6 (three body 6) based on three body chaotic motion. The algorithm slices the data content and superimposes it on the three-body motion as the acceleration changes. Finally the last three-dimensional coordinate positions of the three-body is transformed into a set of hexadecimal numbers as the hash value. After testing, it is confirmed that the algorithm has the output randomness required by the hash function, has better computing performance and occupies less memory space than the standardized hash algorithms such as MD5 and SHA1, and is suitable for edge computing application scenarios such as the Internet of things.

Awards Won:
Association for Computing Machinery: Third Award of $1,500