Randomness improvement of AES using MKP

ABSTRACT

Randomness is a high impact property of the ciphertext that evaluates the strength of a cryptography system. Advanced Encryption Standard (AES) is a symmetric block cipher algorithm that passed the randomness test. AES algorithm is widely used in a computer communication system for securing data transfer. In previous work we proposed a Multiple-key Protocol (MKP) for AES algorithm. In this paper we tested the randomness of MKP-AES algorithm by using the diehard statistical tests software. The randomness of AES is improved when MKP is used.

Keyword: Advanced encryption standard; Diehard; Multiple-key protocol; Randomness; Statistical tests