# Statistical Randomness Testing of Some Second Round Candidate Algorithms of CAESAR Competition

**Authors :** Fatih Sulak, Betül A. Özdemir, Beyza Bozdemir

**Abstract :** In order to improve symmetric key research, several competitions had been arranged by organizations like National Institute of Standards and Technology (NIST) and International Association for Cryptologic Research (IACR). In recent years, the importance of authenticated encryption has rapidly increased because of the necessity of simultaneously enabling integrity, confidentiality and authenticity. Therefore, at January 2013, IACR announced the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR Competition) which will select secure and efficient algorithms for authenticated encryption. Cryptographic algorithms are anticipated to behave like random mappings; hence, it is important to apply statistical randomness tests to the outputs of the algorithms. In this work, the statistical randomness tests in the NIST Test Suite and the other recently designed randomness tests are applied to six second round algorithms of the CAESAR Competition. It is observed that AEGIS achieves randomness after 3 rounds, Ascon permutation function achieves randomness after 1 round, Joltik encryption function achieves randomness after 9 rounds, Morus state update function achieves randomness after 3 rounds, Pi-cipher achieves randomness after 1 round, and Tiaoxin achieves randomness after 1 round.

**Keywords :** authenticated encryption, CAESAR competition, NIST test suite, statistical randomness tests
**Conference Title :** ICSRD 2020 : International Conference on Scientific Research and Development
**Conference Location :** Chicago, United States
**Conference Dates :** December 12-13, 2020