A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map

Hussam A. Ahmed[1] · Mohamad Fadli Zolkipli[1] · Musheer Ahmad[2]

Received: 1 December 2017 / Accepted: 18 May 2018

Abstract

Substitution boxes are essential nonlinear components responsible to impart strong confusion and security in most of modern symmetric ciphers. Constructing efficient S-boxes has been a prominent topic of interest for security experts. With an aim to construct cryptographically efficient S-box, a novel scheme based on firefly (FA) optimization and chaotic map is proposed in this paper. The anticipated approach generates initial S-box using chaotic map. The meta-heuristic FA is applied to find notable configuration of S-box that satisfies the criterions by guided search for near-optimal features by minimizing fitness function. The performance of proposed approach is assessed through well-established criterions such as bijectivity, nonlinearity, strict avalanche criteria, bit independence criteria, differential uniformity, and linear approximation probability. The obtained experimental results are compared with some recently investigated S-boxes to demonstrate that the proposed scheme has better proficiency of constructing efficient S-boxes.

Keywords Substitution box · Firefly algorithm · Discrete chaotic map · Symmetric ciphers