Key dependent dynamic S-Boxes on 3D cellular automata for block cipher

ABSTRACT

Substitution boxes (S-Boxes) are critical components of numerous block ciphers deployed for nonlinear transformation in the cipher process where the nonlinearity provides important protection against linear and differential cryptanalysis. Classical S-Boxes are represented by predefine fixed table structures which are either use for Data Encryption Standard (DES) or Advanced Encryption Standard (AES). Based on cryptanalysis, it does not offer sufficient cipher protections. The S-boxes used in encryption process could be chosen to be key-dependent. For secure communication, we need a better design of S-boxes to be used for encryption and decryption. In this paper we proposed key dependent dynamic 3D cellular automata (CA) S-Boxes for block ciphers. Our work is based on the design of AES S-Boxes which are originally in 2D presentation. The conceptual framework of the 3D CA S-Boxes is to convert and apply the 3D CA rule to static AES S-Boxes. The methodology is to do conversion from the AES S-Boxes into 3D array of (8x8x4) S-boxes, and then applies the 3D CA Von Neumann rules to them. After a 3D array is obtained from the AES S-Box, the 3D CA is applied based on the round key. The 3D array S-Box are then converted back to the 2D array S-Box and finally it is improved to meet the requirements of good S-Boxes. The obtained S-Boxes is called key dependent dynamic 3D CA S-Boxes having interesting features with dynamic stretchy arrangement, which is functionally understood by CA. Our proposed 3D CA S-boxes are better in comparison with the AES S-Boxes with predefined fixed table structures. Experimental results shown that the proposed 3D CA S-Boxes have secure characteristics like nonlinearity, SAC, BIC and algebraic degree. The proposed S-Boxes can be implemented in any block cipher for secure communication.

Keyword: Secure communication; Block cipher; Cellular automata; Dynamic S-Boxes; Key dependent