Iqtadar Hussain* (iqtadarqau@qu.edu.qa), Department of Mathematics, College of Arts, and Science, Qatar University, Doha, Qatar., Doha, 2713, Qatar. Construction of Nonlinear Component for Block Cipher Based on Chaotic Map and Algebraic Structures.

The Advanced Encryption Standard (AES) is widely used in different kind of security applications. The Substitution Box (S-box) is a main component of many modern symmetric encryption ciphers that provides confusion between the secret key and ciphertext. The S-box component that is used in AES is fixed. If we construct this component dynamically, the encryption strength of AES would be greater than before. In this manuscript, we used Chaotic Logistic Map, Mobius transformation and symmetric group $S_{256}$ to construct S-box for AES. The idea behind the proposed work is to make supplementary safe S-box. The presented S-box is analyzed for the following analyses such as; linear approximation probability (LP), nonlinearity (NL), differential approximation probability (DP), strict avalanche criterion (SAC) and bit independence criterion (BIC). The analyses show that the proposed technique is useful in generating high resistance S-box to known attacks. (Received May 02, 2019)