Abstract

S-Box is the only non-linear component in Advanced Encryption Standard (AES) which determines its strength. The Look-Up Table based S-Box of conventional AES occupies large storage space, reduced throughput and consumes more power. This article presents the design of an S-Box based on Reversible Cellular Automata function that reduces the implementation cost. Further, Cellular Automata functions are derived from various rules that are non-linear and S-Box properties are discussed briefly in this paper. With this approach, the time consumption for the AES S-Box is considerably decreased without compromising the non-linearity of conventional S-Box.

References


**Index Terms**

Computer Science

Algorithms
Keywords

AES  Substitution Box (S-Box)  Cellular Automata(CA)  One Dimensional(1-D) CA.