The Memory-Less Method Of Generating Multiplicative Inverse Values For S-Box In AES Algorithm

Abstract

The substitution box (S-box) component is the heart of the Advanced Encryption Standard (AES) algorithm. The S-box values are generated from the multiplicative inverse of Galois finite field GF(2^8) with an affine transform. There are many techniques of gaining the multiplicative inverse values were proposed. Most of the hardware implementations of S-box were using look-up tables (LUTs) (memory-based) to store the values which employ the largest area in design. In this paper, a software method of producing the multiplicative inverse values, which is the generator of S-box values and the possibilities of implementing the methods in hardware applications will be discussed. The method is using the log and antilog values. The method is modified to create a memory-less value generator in AES hardware-based implementation. The implementation is proposed to embed on limited memory, small-sized FPGA.

Author Keywords

AES algorithm; Antilog and log values; Galois finite field GF(28); Memory-less; Multiplicative inverse; Substitution box