Abstract

The DPA attack can efficiently disclose the secret key of an AES Engine easily. To increase DPA Resistant of the AES engine by XORing the generated 16 bit from Pseudo Random Number Generator with the cipher text from the AES Engine. The cipher text is created by AES algorithm which is very Efficient Algorithm for data Securing. The 16 Bit Sequence Generator Circuit also provide Reduction in Area occupied by the Countermeasure circuit and Delay of propagation time by using pipelining process. The Speed of the DPA Countermeasure circuit also increased without degradation in throughput.
Design of 16-bit Countermeasure Circuit with AES Algorithm for AES Engine

References


Index Terms

Computer Science Security

Keywords

Differential Power Analysis (dpa) Ring Oscillators True Random Number Generator
Design of 16-bit Countermeasure Circuit with AES Algorithm for AES Engine

(trng) Pseudo Random Number
Generator (pnr)