Abstract

In the recent past, AES (Advanced Encryption Standard) has been developed to replace DES (Data Encryption Standard) due to several reports of failure [1, 2] of security or key of DES. The replacement has aimed to augment the level of security mainly with the higher key size. Besides the higher level of security, AES has aimed to provide higher efficiency and better flexibility by means of encryption at different levels and with different block sizes [3]. AES, however, suffers from a major limitation owing to error propagation in the encryption process, which is undoubtedly a great research challenge. The AES encryption is done at several rounds of iteration. Each round of iteration has different input data and different key. The input data and the keys of different rounds are all generated from the original source data and the source key respectively. On the basis of this theory the input data and the keys at rounds follow a data path and a key path respectively. Any bit error at any round, if occurs either at the data path or at the key path, the effect propagates and results in remarkably large number of errors. The research [4, 5] reported this limitation of AES in their authoritative work. In literature, several studies have been made on this issue and several techniques are suggested to tackle the effect. In this paper, we have made extensive studies on Error Propagation Effect of AES.
Hybrid Architecture to overcome the Error Propagation Effect of AES

algorithm (data path) and reviewed the solutions provided through an efficient hybrid method so that the error propagation effect of AES can be eradicated. Certainly, there are some assumptions and considerations that are stated in appropriate points of the discussion.

References

- C. T. Bhunia, "Information Technology Network and Internet", New Age International publication, 2005.
Hybrid Architecture to overcome the Error Propagation Effect of AES


Index Terms

Computer Science

Security

Keywords

AES encryption decryption bit error error propagation Longitudinal Redundancy Check

majority rule

Selective encryption