Provably Secure Encryption Algorithm based on Feistel Structure

International Journal of Computer Applications Foundation of Computer Science (FCS), NY, USA

Volume 139

Number 1

Year of Publication: 2016

Authors:

Ahmed M. Rayan, Ahmed A. Abdel-Hafez, Ismail Mohamed Hafez

10.5120/ijca2016908849

Abstract

In 1997 The National Institute of Standards and Technology (NIST) started a process to select a symmetric-key encryption algorithm instead of DES. NIST determined the evaluation criteria that would be used to compare the candidate algorithms depending on the analyses and comments received, NIST selected five finalist algorithms (RC6, MARS, Rijndael, Serpent and Twofish). At the end, NIST selected Rijndael as the proposed Advanced Encryption Standard algorithm (AES). Although Twofish algorithm based on Feistel structure and possesses a large security margin, it has some drawbacks as The Twofish structure is not easy to analyses, the mixing of various operations makes it hard to give a clean analysis and forces us to use approximation techniques. Moreover, The use of key-dependent S-Boxes adds complexity and greatly increase the effort required to write automated tools to search for characteristics (differentials, linear, …) of the structure. In this paper a proposal of a new Secure Symmetric-key Encryption (SSE) algorithm based on Feistel structure is produced to overcome the previous drawbacks and produce a provable secure algorithm.
References

2. P. JUNOD, Statistical Cryptanalysis of Block Ciphers (Lausanne, EPFL, 2005).

Index Terms
Keywords

Symmetric-key cryptography; Block Ciphers; Substitution-Box; Diffusive Components; MDS; branch number.