عنوان مقاله:
A Novel Block Cipher Algorithm with Feistel-Like Structure

محل انتشار:
مجله محاسبات و امنیت, دوره 3, شماره 1 (سال: 1395)

تعداد صفحات اصل مقاله: 14

نویسندگان:
Mahmood Deypir
Yousef Purebrahim

خلاصه مقاله:
Block ciphers have wide applications for hardware and software implementations. In this paper, a new block cipher algorithm with provable security is proposed. The whole structure of the algorithm is novel and has a good encryption and decryption performance. Additionally, it has good security with few number of rounds. The structure of the proposed algorithm consists of ۴-rounds Feistel-Like which uses ۳-rounds Feistel type functions. Moreover, a new method for MDS (Maximal Distance Separable) Matrix construction is proposed and used in the round function as a linear layer. Furthermore, some considerations in S-Boxes of the algorithm lead to obtaining better algebraic expression than AES S-boxes. The Algorithm has a high margin of security against various cryptanalysis methods due to using specific functions in its round functions. Our theoretical evaluations shows that the devised cipher algorithm has provable security against attacks based on linear and differential cryptanalysis and it is robust against differential, truncated differential, boomerang, and integral cryptanalysis in terms of practical security.

کلمات کلیدی:
Cryptography, Cryptanalysis, Practical Security, Provable Security, Cipher Algorithm