New directions in cryptanalysis of block ciphers.

ABSTRACT

The algebraic expression of the Advanced Encryption Standard (AES) RIJNDAEL S-box involved only 9 terms. The selected mapping for RIJNDAEL S-box has a simple algebraic expression. This enables algebraic manipulations which can be used to mount interpolation attack. Approach: The interpolation attack was introduced as a cryptanalytic attack against block ciphers. This attack is useful for cryptanalysis using simple algebraic functions as S-boxes. Results: In this study, we presented an improved AES S-box with good properties to improve the complexity of AES S-box algebraic expression with terms increasing to 255. Conclusion: The improved S-box is resistant against interpolation attack. We can develop the derivatives of interpolation attack using the estimations of S-box with less nonlinearity.

Keyword: Block cipher; AES; S-box; Interpolation attack; Lagrange interpolation formula.