Automatic security evaluation of SPN-structured block cipher against related-key differential using mixed integer linear programming

ABSTRACT

Block cipher algorithms become an essential domain in Information Technology (IT) due to ever increasing the number of attacks. In point of fact, it is significant to produce a security evaluation of block cipher algorithms to determine a statistical non-random behavior of attacks. In relation to this, a new theoretical attack such as related-key differential cryptanalysis (RDC) could give rise to a more practical technique. Basically, estimating immunity of lower bounds in the substitution-permutation network (SPN) block ciphers structure against RDC attack is essential for providing a secure block cipher algorithm. Currently, the automatic computer tools are not applicable to estimate the immunity against related-key differential attacks for SPN block ciphers structure. We present a searching strategy that determines the lower bounds of SPN block ciphers structure against RDC using the Mixed Integer Linear Programming (MILP). This study also aims to demonstrate the applicability and the efficiency of the MILP technique by examining the security of Rijndael block cipher in RDC attack. We prove this technique through calculate the number of activation Sboxes into Rijndael block cipher. The extended MILP technique is able to provide an automatic security estimation tool by giving accurate results. Overall, it is applicable to an extensive variety of block cipher algorithm that makes it an adaptable tool for industrial purposes and scholarly research.

Keyword: Related-key differential cryptanalysis; Mixed Integer Linear Programming (MILP), SPN; Structured block cipher; Rijndael; Automatic search tool