ABSTRACT OF PHD THESIS

Automatic search methods for differential characteristic in relation on cryptanalysis of block ciphers

mgr inż. Władysław Dudzic

This dissertation focuses mainly on differential cryptanalysis and automation of the process of determining the vulnerability of the algorithm to attacks based on differantial techniques. The work proposes an automated search method for optimal differential characteristics (in terms of the minimum number of active substitution boxes or the cumulative maximum probability value) and automated search method for truncated differential characteristics useful for the adversary. The proposed methods use `AIG` graphs to represent the model describing propagation of the differential characteristic or the truncated differentials. The model is generated from an implementation of the function determining the probability of a given differential characteristic, performed in the functional language `Cryptol`. The `AIG` graph representing this transformation is subjected to a functional reduction and then for the purpose of determining a specific form of the characteristic, it is converted to the `SAT` problem, in which the variables representing the differential characteristic are treated as a set of unknowns.

During the conducted research, it was shown that thanks to the proposed approach it is possible to effectively search for differential characteristics. It has been shown that the efficiency of the implemented software based on the proposed method is much higher than in the case of the `CryptoSMT` open source tool. Tests were performed on block ciphers: `AES`, `KLEIN`, `MIDORI`, `PRESENT`, `SPECK`, `SIMON`, `PYJAMASK` and `SATURNIN`. In addition, the properties of `SAT` models (represented as a set of clauses in the `CNF` form) which according to the author assessment affect the time of solving the problem were characterized. The work indicates also a few of previously unknown in the literature differential characteristics determined by the proposed method (e.g the optimal in terms of the maximum probability value differential characteristic for 5 rounds of the block cipher `AES` and 10 rounds of the block cipher `SPECK` with 128 bit block size and optimal in terms of the minimum number of active substitution boxes differential characteristic for 14 rounds of `AES`). The summary of the research indicates also selected by the author the perspective directions of development of the proposed methods.

Keywords: differential cryptanalysis, differential characteristic, truncated differential characteristic, block ciphers, `AIG` graphs, `SAT` solvers.