Linear Approximations Representation of SPN and Feistel Structure Block Ciphers

Shirin Nilizadeh

Computer Engineering and Information Technology Department

Amirkabir University of Technology

The security of block ciphers is assessed through their resistance to known attacks. One of the most important attacks is linear cryptanalysis. The first step in linear cryptanalysis is obtaining an effective linear approximation for the cipher. In this thesis, a model is described for representing the linear approximations of a SPN or DES-like structure cryptosystem through multi-level weighted directed graph, such that the problem of searching for the best linear approximation is equivalent to searching for the minimum weighted path in the directed graph.

There are two steps for constructing the linear approximations representation's graph of block ciphers, first representing the linear approximations of components, then compounding the obtained representing graphs according to the data flow structure of the cipher. At first, we show how to represent the linear approximations for different components used in a block cipher, i.e., linear and non-linear operations, through graphs. Then we introduce four graphs which are used to help combining the linear approximations representation's graph of the components according to SPN and DES-like block cipher's structure. These are "split" graph, "concatenate" graph, "duplication" graph and "XOR" graph. In this way, one round linear approximations representation's graph will be obtained. Finally, by introducing the sequential and parallel combination graphs, the obtained round graphs are combined and the whole space of linear approximations of the block cipher will be represented through a multi-level weighted directed graph. Multi- lane paths are defined in this proposed graph. By tracing a multi-lane path from start node of the graph towards end node of the graph, one linear approximation of the block cipher will be obtained. We proved the correctness of the modeling, and of the joining of the linear approximation graphs of two and more components in sequential and parallel orders. We also proved that each linear approximation for a block cipher is corresponding to a multi- path way in the linear approximation graphs of that block cipher.

We propose "forward- backward" technique to find suitable linear approximations. One active S-Box is considered in the middle round and a linear approximation from the middle round to the last round is found, then another linear approximation from the middle round to the first round is found. Then, the two above linear approximations are joined to obtain a linear approximation from the first round to the last round. We called the procedure of finding the linear approximation from the middle round to the last round as the "forward" procedure and the procedure of finding the linear approximation from middle round to the last round as the "backward" procedure. The linear approximation graph corresponding to encryption algorithm

is employed to find forward linear approximation, and the linear approximation graph corresponding to decryption algorithm is employed to find backward linear approximation.

We also add two virtual nodes, i.e. virtual source node and virtual destination node, to the linear approximations representation's graph of the block cipher. Then, we modify it to obtain a simpler graph. We show the problem of finding the best linear approximation for a block cipher reduces to finding the minimum-weighted path between the two virtual nodes in the proposed graph. The size of this presented graph is $O(n)$*, with respect to n the number of rounds in the block cipher. On the other hand, the size of this graph is* $O(2^m)$*, with respect to m the maximum input/output size of components which are employed in the block cipher. Hence, the size of the search graph is reduced from exponential order to a linear polynomial order, with respect to the numbers of the rounds of block cipher.*

In this thesis, , as a case study, Moamagar block cipher is first represented, then the Ant colony Optimization(ACO) are applied to find the best multi-lane path in linear approximations representation's graph of this block cipher. As a result, we get some efficient linear approximations for this cryptosystem which shows that Moamagar is compromised against a linear cryptanalysis. These obtained linear approximations are much more efficient than the linear approximations which are got from usual way through non systematic searching in other experiences.

Keywords: *linear cryptanalysis of block ciphers, linear approximations, modeling the linear approximations, multi-level weighted directed graph, DES- like structure, SPN structure, Ant colony Optimization.*