

Differential Model of Block Cipher with Ant Colony Technique

Abbas Ghaemi Bafghi
GhaemiB@ce.aku.ac.ir

Babak Sadeghiyan
BaSadegh@ce.aku.ac.ir

Data Security Laboratory, Computer Engineering Department, Amirkabir University of Technology
Tehran, Iran, P.O.Box 15875-4413, Tel. +98 - 021 - 64542739

Extended Abstract

Differential cryptanalysis of block ciphers was proposed by Biham and Shamir. This method of cryptanalysis is done in two phases, which we call them the design and the execution of attack. In the design phase, a cryptanalyst finds weaknesses of a cipher algorithm and applies them to find an appropriate differential characteristic for that cipher. In the execution phase, he must gather enough ciphertext pairs with the found characteristic and then identifies the effective bits of the key according to a counting scheme. These phases can be summarized as the following steps:

I- Design of attack

1. Build the difference distribution table of S-boxes.
2. Compute the probability of all possible one-round characteristics.
3. Examine all combinations of one-round characteristics to find a suitable full-round characteristic.
4. Gather enough cipher pairs with the found characteristic.

II- Execution of attack

1. Gather enough ciphertext pairs with the found characteristic.
2. Identify effective bits of the key.

The bottleneck of the design phase is the step 3, i.e., examining all combinations of the one-round characteristic to find the best full-round characteristic. If these combinations are examined automatically, a more suitable characteristic and in a shorter time may be reached, although even an automated examination may be impractical.

In this paper, we present a new method for finding a suitable differential characteristics based on the examination of all combinations of one-round characteristics and by applying intelligent techniques. The model is presented to find suitable differential characteristics for Serpent, but it can be used for any block cipher. Serpent is a block cipher algorithm with block size of 128 bits and 0~256 bit keys. Its structure is a SP-network, consisting of alternating layers of key mixing, S-boxes and linear transformation.

To compromise the cipher, we should obtain a suitable differential characteristic. Here, we try to have a minimum number of active S-boxes. We start with one active S-box in the middle round, where propagation to forward and backward provided us a suitable result. We call this approach Forward-Backward method. To obtain a suitable full-round characteristic (from the first round to the last round), we consider one active S-box in the middle round and compute a characteristic from the middle round to the first round (Backward) and compute a characteristic from the middle round to the last round (Forward). We composite two above characteristics and obtain a full-round characteristic.

We first implemented the above forward-backward method by dynamic programming and back-tracking technique. Although we managed to obtain suitable result but we spent much time on it, as the examination of all combinations of one-round characteristics is a time consuming task. Then we used ant-colony technique and reached two advantages: Firstly, by applying this approach, one can obtain a suitable result without examining the whole search space. Secondly, intelligent techniques such as Ant colony technique may reduce dependency of cryptanalysis to cryptanalyst. To do this, we developed a model to represent the problem of finding of differential characteristics for a block cipher algorithm to the problem of finding of the shortest path in a directed graph.

By applying our model, we managed to get a better differential characteristics than the published characteristics for Serpent. The results show that this technique has given a better characteristic and in one case gives a characteristic with probability similar to a published paper.

Key words: Cryptography, Block Cipher, Differential Cryptanalysis, Differential Attack, Serpent, and Ant Colony Technique, Optimization.