Crypto Report - 2

Team Anonymous:
CS14B023, Rahul Kejriwal
CS14B039, Bikash Gogoi

Q12. Show formally and with figures and code, the most deadly linear trail in your cipher. Ensure that an attacker would find linear cryptanalysis more difficult than brute force.

A12. We have found the weakest linear trail by taking greedy approach. For first round we find out the input sum output sum pairs for which the bias is maximum. Then for each such pair we find out the input sum for next round by following the active output bits of previous round. For these active bits, we found the output sums for which bias is maximum. For each such output sum we follow the trail to get the active input bits for next round. Similarly we do it for each subsequent round. Finally the trails having maximum bias is the weakest trail.

The net bias found in the weakest linear trail is 1.12263067173e^{-104} (approx 2^{-345}).
Since net bias at the end is less than 2^{-128}, so it is more difficult than brute force.

Attached a file “linear_trail” containing the linear trail.

Q13. Show formally and with figures and code, the most deadly differential trail in your cipher. Ensure that an attacker would find differential cryptanalysis more difficult than brute force.

A13. Our cipher system has a dynamic structure based on the input key. For the purpose of analysis, we will study the purely SPN structure (wherein each of the 20 rounds are of SPN type). The end result we achieve for this structure is made 2^20 = 1048576 times more difficult as the structure of the cipher is variable.

Since the search space of trails is huge (of orders of (2^128)^(no. of rounds = 20) = 10^770), it is impossible to do exhaustive search of differential trails. As approximations, we use greedy techniques for finding worst case trails (for designer).

We considered two approaches:

1. Vanilla Greedy Approach
2. Branching penalized heuristic Greedy Approach

Vanilla Greedy Approach:

We greedily selected the output difference at each activated sbox. Also, the initial input difference was assumed to be only one bit (it is not possible to iterate over all possible input difference as there are $2^{128} = 10^{38.5}$ different initial input differences).

With this framework, we found the worst case trail to have

$$propagation\ ratio\ <\ \text{1e-324}$$

Attached the trail in file ‘vanilla_greedy_diff_trail’.

Branching penalized heuristic Greedy Approach

Consider the ideal differential trail for the attacker: It has only one active Sbox per round (multiple activated Sboxes lead to multiplication of their propagation ratio reducing the net propagation ratio).

In the worst (tractable) case for the attacker, each active Sbox in each round has propagation ratio $1/256\ =\ 0.00390625$ in case of 8x8 sbox. And in such a case, he would have a maximum propagation ratio of differential trail as

$$0.00390625^{20}\ = 6.842277657836021e - 49$$

The aim of any cipher has to be to reduce its maximum propagation ratio to as close to this value as possible (ideally the max propagation ratio would be 0 but that is not realizable).

In order to arrive at such attacker ideal trails we approach the trail search space in terms of a branching penalized heuristic greedy search. In each round, we chose the output difference that minimizes branching and maximizes the propagation ratio:

$$optimization\ function\ = propagation\ ratio\ +\ no\ of\ deactivated\ sboxes\ in\ next\ round$$

Again, for this computation we assume single bit input difference initially (considering all possible input differences is intractable). With this framework, we found worst case differential trail having:

$$propagation\ ratio = 7.52316384526e - 37$$

Taking into account the variable structure effectively:

$$effective\ propagation\ ratio = 7.17464813734054 55e - 43\ = 2^{-140}$$

Hence, differential cryptanalysis is as difficult as brute-force.

Attached the trail in file ‘heuristic_greedy_diff_trail’.

Q14. Revisit all questions in Section 1. If you decide to make changes in any of the answers, mention them here and justify why you are making the changes.

A14. The only change we made was to increase the number of rounds to 20. This was done to make the cipher more secure to differential cryptanalytic attacks.