Report MitM[3]

Irad Nuriel
(324220458/irad_juixanf_2a3cabbd55227e164b5e76bd109cb112edee3d2570dc1e2e5)

April 15, 2021

1) Attack:

    The attack I've implemented is a partial meet in the middle attack, I found that a change in nibbles: 1,2,3, 5,6,7,8,9,10,11,13 of the key doesn't change the 4th nibble of the ciphertext after 3 rounds of TC02 encryption, and that a change in nibbles: 0,1,2,3,4,6,7,10,11 of the key doesn't change the 4th nibble of the plaintext after 5 rounds of TC02 decryption. The attack is an O(2^28 +2^20+2^32) time attack, O(2^20) space, and O(2^16) data.

2) Optimizations/data structures:

    In my implementation I combined the MC and SR in the round function, and moved all the implementation into a cell representation. Also, I used a lot of loop unrolling, and took advantage of the fact that %2^x can be calculated faster with &(2^x-1).

    I used a hash map to store the results of the forward stage(see std::unordered_multimap for more information).

3) Building the program:

    Run make in the folder (see the Makefile for more information).

4) Problems:

    I did not encountered any problems during the solution(only thing was that I first ignored the key scheduler so it didn't work)

5) Extra:

a) I solved both the 7 rounds and the 8 rounds of MiTM against TC02(and with enough time I will be able to solve the 9 rounds with no problem).