Report DummyForce

Eran Lambooij (0123456789/eran__eran_v_)

February 26, 2019

1 Attack

We implemented the DummyForce attack that attacks 6 rounds of the cipher TC01 with 2^{23} computation and 2^{15} memory using 2 plaintext ciphertext pairs.

2 Optimizations/Datastructures

We used a dummyarray (see: dummyarray.c) and we used a different representation of the SBox to increase the speed. This gave us roughly a 30% speedup w.r.t. the reference implementation.

3 Building the program

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

4 Problems

We encountered no problems.

5 Extra

We can use the same attack to attack up to 8 rounds with less than 2^{40} time and 2^{15} memory.