Modelling TC01 in STP

August 18, 2022

We are going to look at the modelling of TC01 (`https://cryptanex.hideinplainsight.io/media/exercise_file/2/specification.pdf`). First we model the propagation of information through the cipher. This can be used to find the key recovery phase of a differential attack or to find a MitM attack.

1 Modelling propagation of information

There are basically three layers to model:

1. Add round key K
2. The linear layer L
3. The Sbox layer S

Exercise 1.1. *Model L and find the maximum number of layers you can propagate.*

Exercise 1.2. *Model S and L and find the maximum numbers of layers you can propagate.*

Exercise 1.3. *Add the key schedule and K in the last model and see how many rounds you can propagate.*

Exercise 1.4 (Extra)**.** *Use the model to find a MitM attack on TC01*

2 Modelling differential propagation

We now turn our attention to propagating differences. The most interesting part of the model is modelling the propagation through the Sbox. To model this propagation we first need to compute the DDT.

Exercise 2.1. *Compute the DDT for the TC01 Sbox*

Exercise 2.2. *Model the propagation through the Sbox.*

One of the problems that you face when modelling the sbox in STP is that we do not have proper access to reals. As such working with probabilities that are not a power of two is hard. For now we treat all 6's in the DDT as if they are 4's.

Exercise 2.3. *Model the differential propagation through TC01, with only power of two probabilities.*

Exercise 2.4 (Extra)**.** *Model the differential propagation through TC01.*

Exercise 2.5. *Find a differential characteristic through TC01 with probability smaller than* 2^{-10}*.*

Exercise 2.6 (Extra)**.** *Combine both models (key recovery and differential) to find a key recovery attack on TC01.*

3 Usefull Links

- `https://smtlib.cs.uiowa.edu/theories-FixedSizeBitVectors.shtml`
- `https://smtlib.cs.uiowa.edu/theories-Core.shtml`