CS553 Cryptography

BitBees

Question 6

In the differential attack described in the class, the characteristic is the propagation of a difference of $(0, 0, 2, 0)$ at each round. This is probabilistic and is done for 4 rounds. A subkey, 4-bits long, of the key of the final layer, k_5, is guessed. Partial decryption occurs and the guess is verified by comparing the symmetric difference of partially decrypted ciphertext and the differential characteristic propagated from the first layer.

$$(0,0,2,0) \underset{\mathrm{R}}{\rightarrow} (0,0,2,0) \underset{\mathrm{R}}{\rightarrow} (0,0,2,0) \underset{\mathrm{R}}{\rightarrow} (0,0,2,0) \underset{\mathrm{R}}{\rightarrow} (0,0,2,0)$$

The probability of the above differential characteristic is:

$$\mathbf{Pr}_{layer_i} = \frac{6}{16}$$
$$\mathbf{Pr} = (\frac{6}{16})^4$$

The important thing to notice is that, there is exactly 1 active s-box in each layer including the fourth. Hence, only a 4-bit long subkey has to be guessed. In order to guess 8 subkey bits in the last round, 2 s-boxes should be active in the last layer. This is possible with the following differential characteristic propagation from layer to layer:

$$(8,0,2,0) \underset{\mathrm{R}}{\rightarrow} (8,0,2,0) \underset{\mathrm{R}}{\rightarrow} (8,0,2,0) \underset{\mathrm{R}}{\rightarrow} (8,0,2,0) \underset{\mathrm{R}}{\rightarrow} (8,0,2,0)$$

The probability of the above differential characteristic is:

$$\mathbf{Pr}_{layer_i} = \frac{6}{16} \times \frac{4}{16}$$
$$\mathbf{Pr} = (\frac{6}{16} \times \frac{4}{16})^4$$