

Homework #3

Differential Cryptanalysis of a 5-round SPN

Consider a **5-round SPN** as studied in the class (also refer to tutorial paper) and perform differential cryptanalysis. The permutation and key mixing steps remains to be same, and the S-box look-up table is the one you selected for linear cryptanalysis (see homework #2). Similarly, generate each sub-key as the three-bit shifted version of the master-key.

Your work should include the following steps.

- Differential characteristics (probabilities) of the custom S-box.
- Selection of the best input/output differential pair.
- Differential characteristic of the SPN.
- Estimation of the overall differential probability

Implementation Aspects: Design the SPN and pick a (16bit) key in random, and generate many plaintext-ciphertext pairs using the selected key, and delete the key without seeing it.

Goal:

- Extract the key using the studied differential cryptanalysis methodology using the known plaintext-ciphertext pairs.
- Present your results in the form of a written report which we will include all the analysis, and experimental results.
- Include the necessary reasoning you have made and provide a discussion on the problems you encountered.

If you have any questions contact me via taha@isis.poly.edu or drop by the room LC-115 before Friday.