SPRING SCHOOL ON SYMMETRIC CRYPTOGRAPHY
EXERCISES DIFFERENTIAL CRYPTANALYSIS

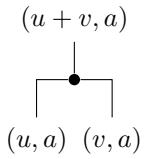
Tim Beyne

11/03/2025

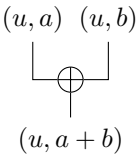
The following exercises accompany the lecture on differential cryptanalysis at the 'Spring school on symmetric cryptography', held on March 11$^{\text{th}}$ 2025. These questions have been designed so they can be solved without computer assistance. Unless stated otherwise, I recommend solving them using pen and paper only.

Questions:

1. Recall that $\mathsf{fork}\colon \mathbf{F}_2^n \to \mathbf{F}_2^{2n}$ is defined by $\mathsf{fork}(x) = x\|x$ and $\mathsf{xor}\colon \mathbf{F}_2^{2n} \to \mathbf{F}_2^n$ is defined by $\mathsf{xor}(x\|y) = x+y$. Prove the propagation rules for the fork and exclusive-or operations in Figure 1.



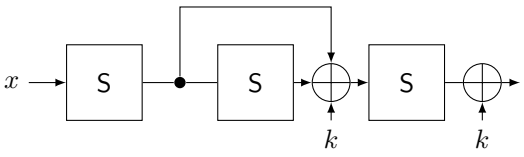
(a) Propagation rule for the fork operation.



(b) Propagation rule for the exclusive-or operation.

Figure 1: Propagation rules for basic operations.

2. In this question you will analyze the construction in Figure 2a. The input of the construction is denoted by x, the secret key by k. The difference-distribution matrix of the S-box S is given in Figure 2b, and its quasidifferential transition matrix is illustrated in Figure 3.



(a) A construction with three S-boxes.

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\
0 & 0 & \frac{1}{4} & \frac{1}{4} & 0 & 0 & \frac{1}{4} & \frac{1}{4} \\
0 & \frac{1}{4} & \frac{1}{4} & 0 & 0 & \frac{1}{4} & \frac{1}{4} & 0 \\
0 & 0 & 0 & 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\
0 & 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & 0 & 0 \\
0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4}
\end{bmatrix}$$

(b) The difference-distribution matrix of S.

Figure 2: Additional information for question 2.

(a) Find a quasidifferential trail with correlation 1/16.

(b) Find a differential characteristic with probability 1/4.

(c) Find a differential with probability one.

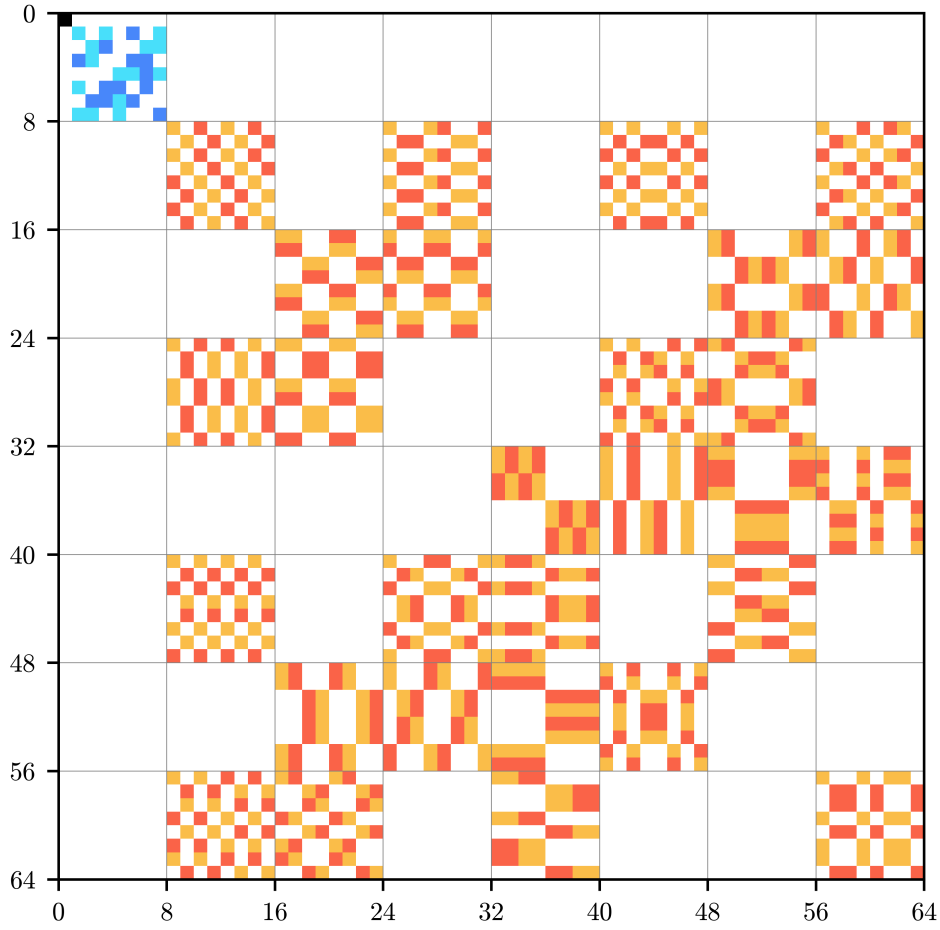


Figure 3: The quasidifferential transition matrix D^{S} of S. Light and dark blue correspond to $\frac{1}{2}$ and $-\frac{1}{2}$ respectively. Yellow and orange correspond to $\frac{1}{4}$ and $-\frac{1}{4}$ respectively.

3. Let $a = \texttt{000000111}$ and $b = \texttt{000011000}$, and denote three rounds of the example cipher by $\mathsf{E}_k \colon \mathbf{F}_2^9 \to \mathbf{F}_2^9$.
   (a) Compute the probability of the differential (a, b) for E_k, as a function of the key k.
   (b) Describe a key-recovery attack on four rounds, and estimate its time- and data-complexity. What is the key-averaged success probability to recover the key uniquely? This is an open-ended question.
   (c) Are the assumptions you made in the previous question really valid? If necessary, use a computer to check — but try to understand the results. Discuss the impact on your estimates.

4. Let $\mathsf{F} \colon \mathbf{F}_2^n \to \mathbf{F}_2^m$ be a function with correlation matrix C^{F} and quasidifferential transition matrix D^{F}. Prove that
$$\sum_{a,b} \left(D^{\mathsf{F}}_{(v,b),(u,a)}\right)^2 = 2^{n-m} \sum_{x,y} \left(C^{\mathsf{F}}_{y,x}\, C^{\mathsf{F}}_{y+v,x+u}\right)^2 .$$
   What does this say for $u = 0$ and $v = 0$?