SPRING SCHOOL ON SYMMETRIC CRYPTOGRAPHY
EXERCISES LINEAR CRYPTANALYSIS

Tim Beyne

11/03/2025

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

Remark. The exercises are based on the following book, to appear in winter 2025:

T. Beyne and V. Rijmen. *Linear Cryptanalysis.* Cambridge University Press.

Questions:

1. Prove the propagation rules for the fork and exclusive-or operations:

$$C^{\mathsf{fork}}_{v_1 \| v_2, u} = \begin{cases} 1 & \text{if } u = v_1 + v_2\,, \\ 0 & \text{else}\,. \end{cases}$$

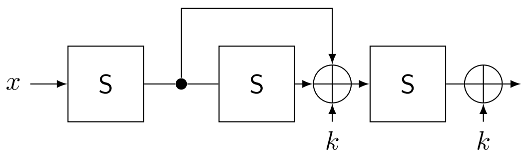
$$C^{\mathsf{xor}}_{v, u_1 \| u_2} = \begin{cases} 1 & \text{if } u_1 = u_2 = v\,, \\ 0 & \text{else}\,. \end{cases}$$

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 $\mathsf{xor}(x \| y) = x + y$.

(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 correlation matrix of the S-box S is given in Figure 2b.
   (a) Find a linear trail with correlation $\pm 1/4$.
   (b) Find a linear approximation with correlation one for at least one key.
   (c) Suppose there exists an x so that the corresponding output is 001. After learning this, and based on your answer to the previous question, what are the possible values of the key?
3. Let $u = \texttt{000000111}$ and $v = \texttt{000011000}$, 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 correlation of the linear approximation (u, v) of 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, assuming the correlation is zero for wrong key guesses? This is an open-ended question.



(a) A construction with three S-boxes.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

(b) The correlation matrix C^{S} of S.

Figure 2: Additional information for question 2.

(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. A fixed point of a function $\mathsf{F} : \mathbf{F}_2^n \to \mathbf{F}_2^n$ is a vector x in $\mathbf{F}_2^n$ such that $\mathsf{F}(x) = x$. Let

$$\mathsf{Fix}(\mathsf{F}) = \left\{x \in \mathbf{F}_2^n \mid \mathsf{F}(x) = x\right\}.$$

Recall that the trace $\operatorname{Tr} A$ of a matrix A is the sum of its diagonal elements. Prove that

$$\#\mathsf{Fix}(\mathsf{F}) = \operatorname{Tr} C^{\mathsf{F}}\,,$$

where C^{F} is the correlation matrix of F.