MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Region of feasible distinguishers). *Let simple hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ be defined through the following distributions of observable outcomes $\mathcal{X}_0$ and $\mathcal{X}_0$:*

$$\Pr\left[x \leftarrow \mathcal{X}_0 : x = x_*\right] = \begin{cases} \frac{4}{42}, & \text{if } x_* \in \{0, \ldots, 3\} \quad , \\ \frac{3}{42}, & \text{if } x_* \in \{4, \ldots, 7\} \quad , \\ \frac{2}{42}, & \text{if } x_* \in \{8, \ldots, 11\} \quad , \\ \frac{1}{42}, & \text{if } x_* \in \{12, \ldots, 17\} \quad , \\ \frac{0}{42}, & \text{if } x_* \in \{28, \ldots, 31\} \quad , \end{cases}$$

$$\Pr\left[x \leftarrow \mathcal{X}_1 : x = x_*\right] = \begin{cases} \frac{0}{42}, & \text{if } x_* \in \{0, \ldots, 3\} \quad , \\ \frac{1}{42}, & \text{if } x_* \in \{4, \ldots, 19\} \quad , \\ \frac{2}{42}, & \text{if } x_* \in \{20, \ldots, 23\} \quad , \\ \frac{3}{42}, & \text{if } x_* \in \{24, \ldots, 27\} \quad , \\ \frac{4}{42}, & \text{if } x_* \in \{28, \ldots, 31\} \quad . \end{cases}$$

Find the region of false positives and false negatives

$$\alpha(\mathcal{A}) = \Pr\left[x \leftarrow \mathcal{X}_0 : \mathcal{A}(X) = 1\right]$$
$$\beta(\mathcal{A}) = \Pr\left[x \leftarrow \mathcal{X}_0 : \mathcal{A}(X) = 0\right]$$

that are achievable by all distinguishing algorithms $\mathcal{A}$. Sketch the region of achievable tradeoffs. Add the naive tradeoff lines based on statistical distance. Explain why the region has symmetry point $(\frac{1}{2}, \frac{1}{2})$. How does the region change if we consider only t-time distinguishers? Does the region preserve symmetry?

Solution.