Exercise Sheet #11

Advanced Cryptography 2021

Exercise 1 Decorrelation

Compute $\|M\|_a$, for

$$M := \begin{array}{c} \\ (0,0) \\ (0,1) \\ (1,0) \\ (1,1) \end{array} \begin{array}{c} \begin{array}{cccc} (0,0) & (0,1) & (1,0) & (1,1) \end{array} \\ \begin{pmatrix} 5 & 4 & 1 & 2 \\ 6 & 8 & 0 & 4 \\ 2 & 4 & 4 & 5 \\ 10 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

where the rows are (x_1, x_2) and the columns (y_1, y_2).

Exercise 2 Decorrelation and Differential Cryptanalysis

A typical measure in the differential cryptanalysis of a random permutation C is the maximum value of the expected differential probability defined by

$$\mathrm{EDP}^C_{\max} = \max_{a \neq 0, b} \mathrm{E}(\Pr_X[C(X \oplus a) = C(X) \oplus b]).$$

Prove that

$$\mathrm{EDP}^C_{\max} \leq \frac{1}{2^m - 1} + \mathrm{BestAdv}_{\mathrm{Cl}^2_a}(C, C^*).$$

Deduce how decorrelation theory can prevent differential attacks.

Exercise 3 Decorrelation (2)

In this exercise we consider a random permutation $C : \{0,1\}^m \to \{0,1\}^m$ and compare it to the uniformly distributed random permutation $C^* : \{0,1\}^m \to \{0,1\}^m$.

1. Prove that $|||[C]^{d-1} - [C^*]^{d-1}|||_\infty \leq |||[C]^d - [C^*]^d|||_\infty$.
   Hint: Use the interpretation of $|||[C]^d - [C^*]^d|||_\infty$ in term of best non-adaptive distinguisher.

2. Prove that $0 \leq |||[C]^d - [C^*]^d|||_\infty \leq 2$.

3. Show that the property $\mathrm{Dec}^d(C) = 0$ does not depend on the choice of the distance on the matrix space.

4. Show that if $\mathrm{Dec}^1(C) = 0$, then the cipher C provides perfect secrecy for any distribution of the plaintext.

In a typical situation, C is a block cipher and the randomness actually comes from the randomness of the secret key. Let $f_K : \{0,1\}^m \to \{0,1\}^m$ be a function parametered by a uniformly distributed random key K in a key space $\mathcal{K}$. We compare f_K to a uniformly distributed random function F^*.

5. Prove that if $\mathrm{Dec}^d(f_K) = 0$, then $|\mathcal{K}| \geq 2^{md}$.

6. Show that for $f_K(x) = x \oplus K$, we obtain $\mathrm{Dec}^1(f_K) = 0$.

7. Propose a construction for f_K such that $\mathrm{Dec}^d(f_K) = 0$ and $|\mathcal{K}| = 2^{md}$.