Notes for Lecture 16 (Draft)

Today we finish the analysis of a construction of a pseudorandom permutation (block cipher) given a pseudorandom function.

Recall that if $F : \{0,1\}^m \to \{0,1\}^m$ is a function, then we define the *Feistel permutation* $D_F : \{0,1\}^{2m} \to \{0,1\}^{2m}$ associated with F as

$$D_F(x, y) := y, x \oplus F(y) \tag{1}$$

Let $F : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^m$ be a pseudorandom function, we define the following function $P : \{0,1\}^{4k} \times \{0,1\}^{2m} \to \{0,1\}^{2m}$: given a key $\overline{K}(K_1, \ldots, K_4)$ and an input x,

$$P_{\overline{K}}(x) := D_{F_{K_4}}(D_{F_{K_3}}(D_{F_{K_2}}(D_{F_{K_1}}(x)))) \tag{2}$$

If $\overline{F} = F_1, F_2, F_3, F_4$ are four functions, then $P_{\overline{F}}$ is the same as the above construction but using the functions F_i:

$$P_{\overline{F}}(x) := D_{F_4}(D_{F_3}(D_{F_2}(D_{F_1}(x)))) \tag{3}$$

If A is an oracle algorithm, we define as $S(A)$ the probabilistic process in which we run a simulation of A in which we reply to each query with a random answer.

The proof of the following result is what was missing from yesterday's analysis.

Lemma 1 *For every non-repating algorithm A of complexity $\leq t$ we have*

$$\left| \mathbb{P}_{\overline{F}}[A^{P_{\overline{R}}, P^{-1}_{\overline{R}}}() = 1] - \mathbb{P}[S(A) = 1] \right| \leq \frac{t^2}{2 \cdot 2^{2m}} + \frac{t^2}{2^m}$$