Exercise. Show that the tree-round Feistel cipher \( \text{FEISTEL}_{f_1, f_2, f_3}(L_0 || R_0) \) is not pseudorandom if the adversary can also make decryption queries.

Solution by Margus Niitsoo

Let \( L_0 || R_0 \) be an arbitrary message. Then the corresponding ciphertexts is

\[
L_3 = R_0 \oplus f_2(L_0 \oplus f_1(R_0)), \\
R_3 = L_0 \oplus f_1(R_0) \oplus f_3(R_0 \oplus f_2(L_0 \oplus f_1(R_0))).
\]

Now the ciphertext of a modified message \( L_0 \oplus \delta || R_0 \) is

\[
L_3' = R_0 \oplus f_2(L_0 \oplus \delta \oplus f_1(R_0)), \\
R_3' = L_0 \oplus \delta \oplus f_1(R_0) \oplus f_3(R_0 \oplus f_2(L_0 \oplus \delta \oplus f_1(R_0))).
\]

As a next step, we can use decryption operation to find \( L_0^* || R_0^* \) such that the corresponding ciphertext is

\[
L_3^* = L_3' \oplus 0 = R_0 \oplus f_2(L_0 \oplus \delta \oplus f_1(R_0)), \\
R_3^* = R_3' \oplus \delta = L_0 \oplus f_1(R_0) \oplus f_3(R_0 \oplus f_2(L_0 \oplus \delta \oplus f_1(R_0))).
\]

By the definition of the Feistel cipher we can express

\[
L_2^* = R_3^* \oplus f_3(L_3^*) = L_0 \oplus f_1(R_0) = L_2, \\
L_1^* = R_2^* \oplus f_2(L_2^*) = R_3^* \oplus f_2(L_2) = L_3^* \oplus f_2(L_2), \\
R_0^* = L_1^* = L_3^* \oplus f_2(L_2).
\]

Similarly, we can derive

\[
R_0 = L_1 = R_2 \oplus f_2(L_2) = L_3 \oplus f(L_2)
\]

and thus we have obtained a relation

\[
R_0^* \oplus L_3^* = f_2(L_2) = R_0 \oplus L_3
\]

that holds with probability 1. The same relation between input and output pairs holds with probability

\[
\frac{1}{2^n - 2}
\]

for random permutation. Hence, the computational difference is really small for the three round Feistel cipher if decryption operations are allowed.