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

Solution by Margus Niitsoo (communicated by Sven Laur)

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

$$\begin{aligned} L_3 &= R_0 \oplus f_2(L_0 \oplus f_1(R_0)) \enspace, \\ R_3 &= L_0 \oplus f_1(R_0) \oplus f_3(R_0 \oplus f_2(L_0 \oplus f_1(R_0)) \enspace. \end{aligned}$$

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

$$\begin{aligned} L_3' &= R_0 \oplus f_2(L_0 \oplus \delta \oplus f_1(R_0)) \enspace, \\ R_3' &= L_0 \oplus \delta \oplus f_1(R) \oplus f_3(R_0 \oplus f_2(L_0 \oplus \delta \oplus f_1(R_0)) \enspace. \end{aligned}$$

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

$$\begin{aligned} L_3^* &= L_3' \oplus 0 = R_0 \oplus f_2(L_0 \oplus \delta \oplus f_1(R_0)) \enspace, \\ R_3^* &= R_3' \oplus \delta = L_0 \oplus f_1(R_0) \oplus f_3(R_0 \oplus f_2(L_0 \oplus \delta \oplus f_1(R_0)) \enspace. \end{aligned}$$

By the definition of the Feistel cipher we can express

$$\begin{aligned} L_2^* &= R_3^* \oplus f_3(L_3^*) = L_0 \oplus f_1(R_0) = L_2 \enspace, \\ L_1^* &= R_2^* \oplus f_2(L_2^*) = R_2^* \oplus f_2(L_2) = L_3^* \oplus f_2(L_2) \enspace, \\ R_0^* &= L_1^* = L_3^* \oplus f_2(L_2) \enspace. \end{aligned}$$

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.

Exercise. Show that collision resistance does not follow from second preimage security for compressing hash function families.

Solution by Margus Niitsoo (communicated by Sven Laur)

Let $\mathcal{H}$ be a compressing hash function family that is (t, ε)-secure against second preimage attacks. Let m_0 and m_1 be two distinct inputs in the message space and y_0 be a plausible output. Then for any hash function $h \in \mathcal{H}$, we can define modified hash function

$$h^*(m) = \begin{cases} y, & \text{if } m = m_0 \enspace , \\ y, & \text{if } m = m_1 \enspace , \\ h(y), & \text{otherwise} \enspace . \end{cases}$$

The corresponding hash function family $\mathcal{H}^*$ is $\bigl(t, \frac{2}{|\mathcal{M}|} + \varepsilon\bigr)$-secure against second preimage attacks. The game chain depicted below provides a formal proof

$\mathcal{G}_0^{\mathcal{A}}$	$\mathcal{G}_1^{\mathcal{A}}$
$h \xleftarrow{u} \mathcal{H}$,	$h \xleftarrow{u} \mathcal{H}$,
$x_0 \xleftarrow{u} \mathcal{M}$	$x_0 \xleftarrow{u} \mathcal{M}$
$y \leftarrow h(x_0)$	$y \leftarrow h(x_0)$
if $x = m_0$ then $y \leftarrow y_0$	if $x = m_0$ then $y \leftarrow y$
if $x = m_1$ then $y \leftarrow y_0$	if $x = m_1$ then $y \leftarrow y$
$x_1 \leftarrow \mathcal{A}(h, x_0)$	$x_1 \leftarrow \mathcal{A}(h, x_0)$
if $x_0 = x_1$ then return 0	if $x_0 = x_1$ then return 0
return $[h(x_0) \stackrel{?}{=} h(x_1)]$	return $[h(x_0) \stackrel{?}{=} h(x_1)]$

since $\mathcal{G}_0$ and $\mathcal{G}_1$ are the security games that quantify second preimage resistance of the function families $\mathcal{H}^*$ and $\mathcal{H}$. Now note that the hash function family $\mathcal{H}^*$ is not collision resistant, as a fixed pair (m_0, m_1) is sufficient to create collision for all functions of $\mathcal{H}^*$.

An explicit example. Let $\mathcal{H}_{\mathrm{all}} = \{h : \{0,1\}^n \to \{0,1\}^m\}$ be a family of all hash functions and let $m_0 = 00\ldots0$ and $m_1 = 11\ldots1$. Then we get the desired separation between collision resistance and second preimage resistance, since $\mathcal{H}_{\mathrm{all}}$ is collision resistant for all reasonable time bounds.