

ENEE 459E/CMSC 498R: Introduction to Cryptology  
CRHF Class Exercise 3/9/17

Let  $(Gen, H)$  be a collision-resistant hash function and let  $F$  be a PRF. For each of the following, state whether  $\hat{H}$  is necessarily collision resistant. Justify your answer.

1.  $\hat{H}^s(x_1||x_2) = H^s(x_1 \oplus F_s(x_2))$

2.  $\hat{H}^s(x_1||x_2) = H^s(H^s(x_1)||x_2)$