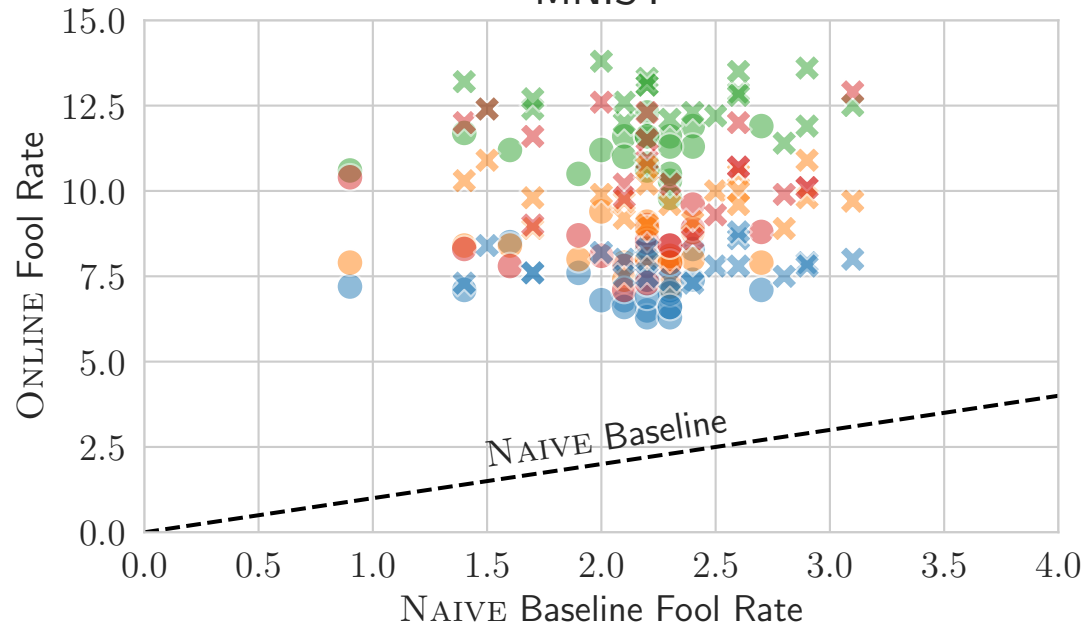
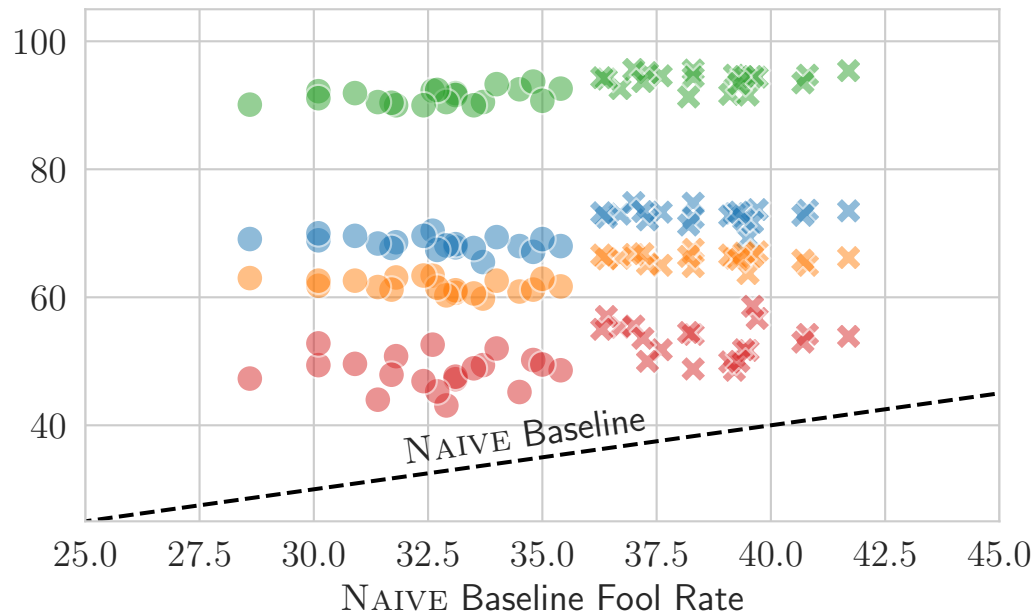


MNIST



CIFAR-10



■ VIRTUAL   
 ■ OPTIMISTIC   
 ■ VIRTUAL+   
 ■ SINGLE-REF   
 ● FGSM Attack   
 × PGD Attack