deep MLP · MNIST .00 .01 .02 .03 .04 .05 .06 .07 .08 .11 .12 .13 .14 .15 .16 .17 .18 .19 acc. FGSM attack 0.5 0.0 acc. PGD attack 0.5 α CNN · MNIST .02 .03 .04 .05 .06 .07 .08 .09 .10 .12 .13 .14 .15 .16 .17 .18 .19 .00 .01 .11 acc. FGSM attack 0.5 0.0 acc. PGD attack 0.5 α α CNN · CIFAR-10 .06 .00 .01 .02 .03 .04 .05 .07 .08 .09 .10 .11 .12 .13 .14 .15 .16 acc. FGSM attack 0.3 0.0 acc. PGD attack 0.3 0.0 α α