

ML2021Spring HW10 Report

NTNU ME 吳政彥

40673034H

| Public Score | Private Score |
|--------------|---------------|
| 0.000 | 0.010 |

The methods I used to pass the strong baselines include:

1. Use 11 pretrained models to ensemble (Including resnet110_cifar10, wrn40_8_cifar10, preresnet110_cifar10 and so on)
2. Sum up the output of 11 pretrained models, and then use CrossEntropyLoss to calculate the probability of each label
3. Decreasing alpha to $2 / 255 / \text{std}$
4. Use IFGSM to attack this ensemble model with $\text{num_iter} = 20$