**ML2021Spring HW10 Report**

Material Science and Engineering Hou, Yu-Chien

B08507012

|  |  |
| --- | --- |
| **Public Score** | **Private Score** |
| 0.020 | 0.010 |

The methods I used to pass the boss baselines include:

1. I performed ensemble attack by calculating the loss on the average of different models’

prediction label in the fgsm() function.

1. I used ifgsm as my attacking algorithm, and I modified the gen\_adv\_examples() function

similarly to the fgsm() function, that is averaging the prediction labels before calculating

the loss.

1. I tried multiple combinations of 5 models for ensemble attack, and found out that models

with the resnet110 suffix perfomed better together. The models I chose were：

1. resnet110\_cifar10
2. preresnet110\_cifar10
3. seresnet110\_cifar10
4. sepreresnet110\_cifar10
5. diaresnet110\_cifar10