

ML2021Spring HWX Report

<Department> <Name>

<Student ID>

Public Score	Private Score
0.040	0.040

The methods I used to pass the strong baselines include:

1. Change the ifgsm to mifgsm. You should add a constant μ to calculate g before you get x_{adv} . ($g_0 = \mu * g_0 + x_{adv}.grad.detach()$, $x_{adv} = x_{adv} + \epsilon * g_0.sign()$)
2. You should choose several models to ensemble. I choose 7 models which you can see in the source code. After that, you may run every model and sum their loss and y_p to become new loss and y_p .