FREE VS FAST ADVERSARIAL TRAINING

A PREPRINT

Giuseppe Capaldi
University of Rome "La Sapienza"
capaldi.1699498@studenti.uniroma1.it

Gianluca Capozzi
University of Rome "La Sapienza"
capozzi.1693255@studenti.uniroma1.it

September 22, 2020

ABSTRACT

1 Introduction

2 Adversarial Machine Learning

3 PGD attack

4 Free Adversarial training for free!

5 Fast is better than free

6 Conclusions