华 北 电 力 大 学

2014 届　计算机科学与技术_专业毕业设计（论文）答辩记录表

学生姓名 孙昱伟_　学号 201409010119　专业班级 计算机科学与技术 1401

毕业设计(论文)题目 深度学习中的生成对抗网络攻击设计与实现

所提问题及回答情况：

问题一：这个协同学习网络采用的是什么模型。

回答：采用三层架构模型，每层分别有 784，300，150 个神经元。

问题二：上传与下载的参数是全部下载吗。

回答：目前是全部下载，下一步可以考虑采用合适的算法来实现有选择性地进行参数的上传及下载。提高 GAN 模型还原其他用户数据的效率及精确度。

问题三：这个三层架构网络还可以采用别的网络模型吗，比如 CNN。

回答：是的，可以试着在生成器及判别器内采用学习精度更好的像 CNN（卷积神经网络）等神经网络模型，提高还原图像的真实性。比如可以考虑采用 DCGAN（深度卷积对抗神经网络）。

记录人：

年　月　日