中文论文题目：面向差分隐私机器学习算法的研究与评估

英文论文题目：**Research and Evaluation System Development for Differentially Private Machine Algorithms**

机械或

工业设计工程或软件工程或人工智能

提交日期　2023 年 7 月 10 日

目录

1　已完成的论文工作及取得的阶段性成果

1.1　总体工作进展

1.2　各章节完成情况及取得的阶段性成果

摘要

第一章，绪论

第二章，相关理论基础

第三章，差分隐私算法的分类研究

第四章，评测框架设计与实现

第五章，算法评测结果及分析

第六章，总结与展望

2　下一步论文工作安排

2.1　重难点分析及拟采取的解决措施

难点 1. 如何实现评测框架的高可扩展性？

解决措施

难点 2. 差分隐私训练算法时间开销大

解决措施

3　目前取得的成果

正在进行中