

成绩评定

■ 课程最终成绩 = 平时成绩（40%）+ 期末考察成绩（60%）

■ 平时成绩： 40%

- 课堂考勤与参与（10%）
- 两次作业（各占15%）

■ 期末考察成绩： 60%

期末考察以课程报告的形式进行。学生可从以下两类选择其一完成：

- 文献阅读报告。在规定论文列表中选择2篇进行综合文献阅读，将阅读学习结果以文字报告报告形式呈现。
- 芯片安全实验报告。通过简单芯片测试或芯片安全仿真实验，培养同学们的实践动手能力。

文献阅读报告要求

- 一个报告，两个部分。每个部分对应一篇论文阅读报告。
- 每篇论文阅读报告不少于2页纸；报告不少于4页纸；
- 阅读报告总字数不少于4000字
- 每篇论文的阅读报告至少包括三个部分，
 - 概述：
 - 结构与内容分析：
 - 优缺点评价：

文献阅读报告要求

1. **论文概述：**对所读学术论文进行简要概述，包含论文题目、作者、发表时间、研究背景、研究目的、研究方法等。

2. **论文结构与内容分析：**

1) **结构分析：**分析论文的结构，包括引言、文献综述、研究方法、研究结果、讨论与结论等各部分之间的逻辑关系。

2) **内容分析：**针对论文的每个部分进行深入的内容分析。如，引言部分阐述论文的研究背景、研究目的和研究意义；方法部分详细介绍论文所提出的方法；实验部分展示实验数据来源、图表、结果分析比较等。

3. **论文优缺点评价：**对研究进行深入讨论，阐述研究发现的实际意义和理论价值。对论文的优缺点进行客观评价。优点可以包括论文的创新性、研究方法的严谨性、论证的合理性等；缺点可以包括论文的局限性、研究方法不足、论证不充分等。

L

7

└

7

文献阅读报告要求

- ❑ 有 A/B/C三大类，A类里面有13篇论文，B类有11篇论文，C类有12篇论文。
- ❑ 要求每人选2篇论文阅读。其中每类限选1篇。
- ❑ 每篇论文最多只能被选4次。
- ❑ 根据发在QQ群内的论文阅读清单，将选择告诉助教，如 A10B9、B2C11… 最晚不晚于11月6日下午17:30。

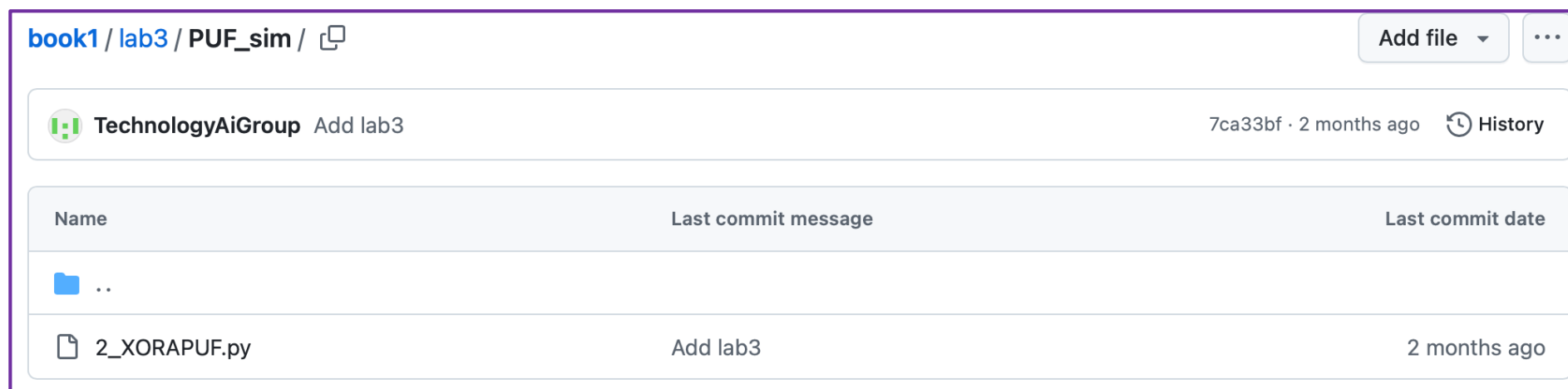
芯片安全实验报告要求

1、PUF仿真实验：

请实现64bits， 6-XOR APUF， 在给定challenge或者 Φ 时， 能够得到正确响应值。

芯片安全实验报告要求

在对基于APUF的PUF设计进行仿真时，其核心的步骤在于利用LAD模型构建APUF的行为逻辑，并在此基础上完成PUF的响应输出。以128bits，2-XOR APUF为例，课程网站用Python实现的CRP仿真核心代码已给出如下：



https://github.com/TechnologyAiGroup/book1/tree/main/lab3/PUF_sim

芯片安全实验报告要求

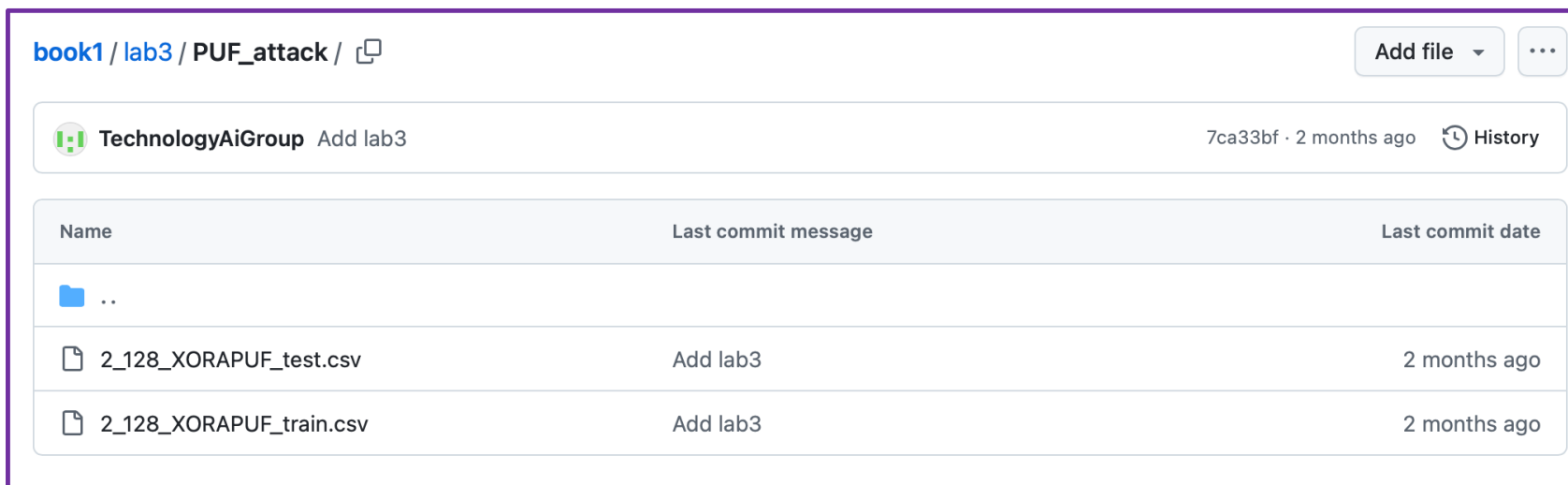
2. 建模攻击实验:

请利用逻辑回归（Logistic Regression），或者其他机器学习算法，对128bits 2-XOR APUF进行机器学习建模攻击。利用给出的数据集进行训练，在测试集上得到90%以上的正确率。

芯片安全实验报告要求

基于目标PUF的原理，攻击者可构建包含待训练参数（如PUF中weight）的PUF模型。基于CRP数据集，利用LR算法训练参数，完成对目标PUF的机器学习建模攻击。

目标PUF的数据集在课程网站中提供，其中challenge已经被处理转换为 Φ 。每一行为一条CRP数据，包含130个数。其中前129个数为 ± 1 ，代表 Φ ；最后一个数为0或1，代表响应值。



The screenshot shows a GitHub repository interface for the path `book1 / lab3 / PUF_attack`. The repository is owned by `TechnologyAiGroup`. The commit hash is `7ca33bf` and it was updated 2 months ago. The file list includes a parent directory `..` and two CSV files: `2_128_XORAPUF_test.csv` and `2_128_XORAPUF_train.csv`, both committed with the message "Add lab3" 2 months ago.

Name	Last commit message	Last commit date
..		
2_128_XORAPUF_test.csv	Add lab3	2 months ago
2_128_XORAPUF_train.csv	Add lab3	2 months ago

https://github.com/TechnologyAiGroup/book1/tree/main/lab3/PUF_attack

课程报告要求

- 选择“文献阅读报告”的同学。
请用“课程报告-文献阅读-模板”
- 选择“芯片安全实验报告”的同学，
请用“课程报告-芯片实验-模板”
并在后面附上代码