王晶晶

女/2002.07

13336016402

3200104880@zju.edu.cn

https://23wjj.github.io

https://github.com/23wjj

基本信息

浙江大学 - 信息安全（辅修金融学） **2020.09 - now**

- GPA 4.73/5.0 (3.99/4.0)
- 排名 五学期专业第一

  semester Ⅰ - 2/725 工信大类

  semester Ⅱ - 1/27 信安专业
- 英语能力

  CET4-588

  CET6-593
- 专业课程
  - 23/53门课程满绩（95+)

    计算机系统Ⅰ/Ⅱ/Ⅲ，计算机系统概论，程序设计专题，面向对象程序设计，数据结构基础，微积分，线性代数，常微分方程，大学物理，软件安全，密码学，信息与电子工程导论
  - 40/53门课程90+

    计算机网络，高级数据结构与算法分析，微观经济学，公司金融，面向信息安全的信号处理
  - 成绩单另附

荣誉奖项

- 奖学金

  2020-2021学年浙江大学二等奖学金

  2021-2022学年国家奖学金

  2021-2022学年乐信圣文科研创新奖学金

- 科研竞赛

  2021年浙江省大学生高等数学竞赛二等奖

  第十三届全国大学生数学竞赛（非数学类）省级一等奖

  第六届全国大学生计算机系统能力培养大赛（龙芯杯）团体赛二等奖

项目经历

1. 基于Chisel的Mips32处理器开发

chisel verilog mips32

- **项目描述**

  MMM (Marvelous MIPS Machine) 是一款基于 Chisel 语言开发的 MIPS32 架构处理器，采用顺序双发射五级流水线，在龙芯实验箱上的频率可达 110MHz。

- **项目内容**
  - MMM 总体结构分为处理器核心、数据缓存、指令缓存、总线仲裁转换器。其中处理器内部分为前后端，前端包含两个阶段，分别为 IF 和 ID，后端包含三个阶段，分别为 IS, EX 和 WB，共五级流水线。
  - 在设计时着重优化了运行过程中最为严重的性能瓶颈：分支预测。MMM 处理器采用了基于 BHT+BTB 的经典分支预测器，在性能测试中平均分支预测准确率可达88.24%，使得性能测试达到了 87.830 分。
  - MMM 处理器适配 PMON、uCore 和 Linux 操作系统

2. Defending Data Inference Attacks against Machine Learning Models by Mitigating Prediction Distinguishability

python

- **项目描述**

  通过减小训练集成员和非训练集非成员在深度学习模型输出上的差异性来防御成员推断攻击、对抗样本攻击、属性推理攻击、模型逆向攻击等经典的推断攻击。在cifar10、cifar100、facescrub530、texas、location、purchase100等经典数据集上都取得了良好的效果。

- **项目内容**
  - 核心是一个CVAE，以标签作为条件学习非成员数据的特征分布，从而减小成员与非成员输出结果上的差异性
    - Purifier引入label swapper来抵御新型的成员推断攻击，即label-only attack
- **项目成果**

  TDSC 在投

3. Distribution Inference against Generative Models

- **项目描述**

  Stable Diffusion等新型生成模型的提出，正在逐渐取代传统的GAN。但相较于GAN，扩散模型存在更大的隐私泄露的风险。研究提出一种对于生成模型的基于数据分布粒度的新型攻击。

- **项目成果**

  CCS（二作）在投