导引课

1. 授课内容

- 第一章 数据安全概述
- 第二章 密码基础
  - 2.1 基础知识
  - 2.2 对称密码
  - 2.3 公钥密码
  - 2.4 可证明安全性*
  - 2.5 通用可组合安全*
- 第三章 同态加密
  - 3.1 基本概念
  - 3.2 半同态Paillier方案
  - 3.3 类同态BGN方案
  - 3.4 全同态典型方案
  - 3.5 开发框架SEAL
- 第四章 典型密码原语
  - 4.1 承诺
  - 4.2 零知识证明
  - 4.3 秘密共享
  - 4.4 茫然传输

密码技术篇

14课时

补充密码知识

（兼顾计算机专业）

介绍密码原语

（强化密码知识）

- 第五章 隐私保护的数据发布
  - 5.1 基本概念
  - 5.2 K-匿名模型
    - 5.2.1 K匿名
    - 5.2.2 l-多样化
    - 5.2.3 T-相近
    - 5.2.4 其它模型
  - 5.3 数据脱敏与溯源
    - 5.3.1 数据脱敏
    - 5.3.2 数据溯源
  - 5.4 保留格式加密及应用
- 第六章 差分隐私
  - 6.1 基本概念
  - 6.2 拉普拉斯机制
  - 6.3 指数机制
  - 6.4 随机响应机制
  - 6.5 差分隐私应用
    - 6.5.1 Google RAPPOR模型
    - 6.5.2 Google ESA模型
    - 6.5.3 基于图模型的数据合成
    - 6.5.4 直方图发布方案设计

数据发布篇

4课时

保留格式加密

（强化密码知识）

隐私数据发布

差分隐私

1. 授课内容

第六章 密文查询

- 6.1 可搜索加密
  - 6.1.1 基本概念
  - 6.1.2 对称可搜索加密
  - 6.1.3 非对称可搜索加密
- 6.2 保留顺序加密
  - 6.2.1 基本概念及构造
  - 6.2.2 顺序揭示加密
- 6.3 频率隐藏保序加密
  - 6.3.1 典型构造
  - 6.3.2 UDF示例
  - 6.3.3 FH-OPE实现
- 6.4 密态数据库
  - 6.4.1 基本概念
  - 6.4.2 CryptDB数据库

数据查询篇

6课时

密文查询

密态数据库

第七章 密文集合运算

第八章 安全多方计算

- 8.1 布尔电路
  - 8.1.1 姚氏百万富翁问题
  - 8.1.2 混淆电路构造思想
  - 8.1.3 姚氏乱码电路协议
  - 8.1.4 电路优化
- 8.2 算术电路
  - 8.2.1 姚氏百万富翁问题
  - 8.2.2 ABY框架及应用实践

第九章 不经意随机存取模型

- 9.1 基本定义
- 9.2 典型构造
- 9.3 多云ORAM

第十章 联邦机器学习

- 10.1 联邦学习
- 10.2 横向联邦学习
- 10.3 纵向联邦学习

数据计算篇

8-10课时

密文交集运算

安全多方计算

隐私机器学习

访问模式保护

每章精心设计小实验
每篇设计综合大实验

2. 考核方式

100%平时成绩

课堂表现

出勤情况：10分，迟到一次扣0.5、旷课一次扣1分、无故旷课3次本课程不通过

课堂考核：实时答题，30分

实验报告

45分，抄袭一次扣5分、晚交一次扣1分，其他根据实验报告内容和完成情况给予相应分数

分组作业

论文解读汇报：15分，每一组从10篇论文中选一篇识读、期末汇报答辩，给分数

2. 考核方式

论文解读

制作PPT，汇报论文的主要动机、主要贡献、主要方法和实现效果，汇报时长为10分钟；汇报基于该论文的后续可以开展的工作以及思路，时长不超过5分钟。

根据汇报情况得0-12分；每位同学有3分抽查回答分数。

每组要求：每组4-5人

参照软件安全课程方式

谢　谢