**培训题目**

实用化隐私保护计算协议的设计

**内容摘要**

讲座介绍面向现实世界应用的同态加密、零知识证明和安全多方计算，并展示如何综合以上密码工具设计实用化的隐私保护计算协议。

Part 1: 零知识证明及其在隐私保护密码货币中的应用

* Sigma协议的通用构造范式VSS-in-the-Head
* 账户模型下隐私保护的密码货币的设计与实现

Part 2: 隐私集合运算协议的设计

* 隐私集合运算协议概览
* 隐私集合求并协议的设计
* 隐私集合运算统一构造框架的设计与实现
* 隐私集合运算的非平衡与多方扩展

**个人简介**

陈宇，山东大学网络空间安全学院教授, 博士生导师。主要研究方向是密码学的理论与应用，近年聚焦零知识证明与专用多方安全计算协议。以第一或通讯作者在密码与安全领域的国际顶级会议CRYPTO、ASIACRYPT、PKC、ACM CCS、USENIX Security等和顶级期刊Journal of Cryptology等上发表论文多篇, 主持承担国家自然科学基金多项, 获2018中国密码学会密码创新奖二等奖，蝉联2020、2022央行金融密码杯创新赛最高奖，2022入选《麻省理工科技评论》中国隐私计算十大科技创新人物。

