**实习**

* 背景：在华为2012实验室，职位为隐私保护工程师，主要研究方向为隐私保护机器学习（包括大模型的隐私推断与训练）。
* 实习任务：
  + 调研了业界主流的机密计算框架（微软的EzPC，蚂蚁的SecretFlow，华为的Bicoptor），对它们的性能做了benchmark测试。
  + 设计高效安全的分布式比较函数
  + 实现并测试端到端的安全大模型推断系统
* 实习工作：
  + 阅读了微软EzPC项目，蚂蚁SecretFlow项目和华为Bicoptor项目的论文
    - 结合他们论文中的想法设计了更高效的协议
      * 确定性的截断协议
      * 利用FSS的分布式比较函数
    - 在密码学方面和GPU方面都有效率的提升
      * GPU的AES算法加速
  + 基于上述协议进行了具体的代码实现
    - 在不同的带宽（5GB，1GB，500MB）和批处理大小下测试了最底层比较函数的开销（1ms）
    - 在不同的带宽（5GB，1GB，500MB）和批处理大小下测试了端到端的VGG16模型的开销（10s左右），数据集为CIFAR10。

**双层一体安全高性能区块链智能合约语言关键技术研究**

* 项目背景：是国家重点研发计划“区块链”重点专项项目，研究领域模型及智能合约领域特定语言族。采用分层设计的理念构建语言族框架。将DSL分为表达层、知识层、语义层。表达层简化智能合约编码过程，知识层抽象和封装领域知识，语义层提供不同领域的DSL可组合和扩展的模型，设计面向金融、政务、民生等领域的DSL。
* 项目任务：
  + 领域模型及智能合约领域特定语言族设计
    - DSL的语法应该易于理解和记忆，同时应该与领域相关的术语和概念保持一致。
    - 此外，语法应该允许用户轻松地表达其意图，同时减少可能出现的错误。
  + 智能合约代码合成与转译技术
    - 一是如何支持针对新领域设计的DSL编写的智能合约在区块链上运行，
    - 二是如何使DSL编写的智能合约能够高效运行，
    - 三是如何支持DSL和新型通用智能合约编程语言编写的智能合约交互，
    - 四是如何保证通过DSL编写的智能合约的正确性和安全性。
* 项目工作：
  + 民生领域的模型构建：调研了大量区块链在民生领域的应用场景，
    - 医疗方面：促进医疗行业数据互联互通，构建疾病专科专病可信数据联合循证分析平台。
    - 农生方面：产业数据采集和管理功能
  + 民生领域的语言设计：我发现民生领域中与区块链结合最紧密的应用为医疗健康，其涉及病人数据的共享与隐私计算。因此我对智能合约上最常用的隐私计算算法进行了建模，并设计了隐私计算DSL—CryptLang。
    - 语义拆分：流程语义+隐私计算语义
    - 密码学任务调研
    - CryptLang设计
    - 编译器实现
    - 安全性检测
* 项目成果：
  + 简单实用的语言
  + 实际落地的应用示范

**非开源联盟链基础平台**

* 项目背景：围绕联盟链在国产密码应用、高隐私保护等方面的短板，研究密钥管理、身份认证、数据加密等基于国产密码的链内多维度安全保护技术方案，支撑国家核心领域应用的高安全和隐私保护要求。
* 项目任务：研究基于群签名的通用场景身份与密钥管理技术，支持用户的动态加入及恢复，保证用户的身份、用户属性以及场景要求设计不同粒度的数据访问控制，设计基于属性的身份管理技术，实现灵活的访问控制。
* 项目工作：
  + 去中心化访问控制的协议设计
    - 我设计了一个同时保证身份，数据和访问策略安全的系统
    - 包括身份签发方，用户，服务提供方，访问控制委员会
  + 访问公平性和策略隐私性的实现
    - Time lock puzzle
    - 混淆电路，零知识证明

**Heimdall: Decentralized Access Control Scheme Enabling Fair Access and Policy Confidentiality.**

* **分布式访问控制的概念**：
  + 分布式访问控制（DAC）是在没有单一控制实体的情况下管理访问权限。
  + 基于区块链的DAC利用区块链的分散和透明特性，对个人数据进行可验证的控制。
* **现有方法的局限**：现有的方法主要关注智能合约的访问控制，未能实现公平访问和策略机密性。
* **Heimdall方案的提出**：
  + 提出了一种新的基于区块链的DAC方案，名为Heimdall，实现了公平访问和策略机密性，并提供面向服务的访问控制。
  + Heimdall利用公开可验证时间秘密共享（PVTSS）来规范秘密共享和重构的过程，解决公平访问问题。
  + 采用混淆电路方案和零知识证明来实现策略机密性，同时保证用户身份的机密性。
* **实现与功能**：Heimdall使用功能加密、可验证加密和基于令牌的身份验证分别实现计算、验证和授权服务。实现了Heimdall的原型，并展示了其实验结果，证明其具有实际性能。

**DIDAPPER: Practical and Auditable On-Chain Identity Service for Decentralized Applications.**

* 现有DID系统的局限性：许多现有的DID系统缺乏完整的可审计性和与去中心化应用的互操作性，这限制了它们的实际应用。
* DIDAPPER的解决方案：为了解决这些限制，DIDAPPER提出了一个实用的链上身份服务。它利用群签名为链上用户和去中心化应用提供匿名且可追踪的凭证。
* DIDAPPER的目标：系统旨在确保匿名性、可审计性和服务化。重点在于在保障用户隐私的同时确保符合监管要求的可追踪性，并且高效灵活地服务广泛的去中心化应用。
* 系统参与者：论文概述了DIDAPPER系统中不同类型的参与者，包括DIDAPPER服务、群管理者、去中心化应用（Dapp）和用户。
* 工作流程和协议：详细讨论了诸如群创建、认证、密钥分发、凭证使用与验证以及凭证追踪等详细的工作流程过程。
* 性能和功能性评估：论文评估了DIDAPPER在以太坊平台上的性能，强调了链上验证的效率以及为实现匿名性和可审计性所引入的开销的可接受性。

**CRYPTCODER: An Automatic Code Generator for Cryptographic Tasks in Ethereum Smart Contracts.**

* 问题背景：以太坊为智能合约提供了一系列系统级别的加密API，以便进行各种加密操作。然而，由于缺乏加密领域专业知识，开发者在使用这些低级API时常常遇到难题，从而产生不安全的代码。
* CRYPTCODER的介绍：为解决这个问题，研究者们引入了CRYPTCODER，一个自动代码生成器，用于桥接低级加密API和高级加密任务之间的差距。开发者可以使用CRYPTLANG轻松且安全地实现签名和承诺等加密任务，并利用CRYPTCODER将其自动转换成Solidity代码。
* CRYPTLANG的特性：CRYPTLANG是一个基于任务的语言，支持三种以太坊中常用的加密类别：承诺、签名和摘要。它允许开发者专注于加密任务的高级规范，定义所使用的加密方案。CRYPTCODER能够自动将这些高级规范转换为Solidity实现。
* CRYPTCODER的组件：包括解析器（用于解析输入的CRYPTLANG代码）、辅助模板（提供必要的代码输入以保证输出代码的功能性）以及集成器（将抽象语法树与辅助模板合并，自动生成Solidity代码）。
* 功能评估：对CRYPTCODER进行的评估显示了其在生成Solidity代码方面的功能性，以及相对于参考代码仅增加了4%的平均气体成本的可接受开销。
* 结论和未来工作：论文指出，CRYPTCODER为开发者有效处理高级加密任务提供了帮助，虽然增加了一定的气体开销，但仍是可接受的。未来的工作将包括扩展CRYPTCODER支持的加密代码类别范围，并增强其包括自动生成链下JavaScript代码的能力。

**A Sharding Blockchain-based UAV System for Search and Rescue Missions.**

* 区块链与无人机的结合：论文讨论了将区块链应用于无人机（UAV）搜索与救援（SAR）任务中的优势。特别强调了区块链在提高系统安全性和去中心化决策方面的作用。
* 区块链可扩展性的挑战：尽管区块链提供了多种优势，但其在可扩展性方面存在限制。随着网络参与者数量的增加，区块链的吞吐量可能会快速下降。
* 分片技术：论文提出分片技术作为解决区块链可扩展性问题的方案。通过将区块链网络分成独立运行的小分区（分片），使得系统能够支持大量的搜索与救援无人机。
* 动态分片机制：除了分片带来的可扩展性优势外，系统还通过动态创建可配置的、专门用于任务的分片来提高适应性，并通过支持不同分片间智能合约的调用来提高互操作性。
* 系统实现与评估：论文还描述了该系统的实现原型，包括对提高适应性和互操作性的分析，并进行了性能评估。结果表明，该系统能够实现目标，克服了基于区块链的无人机系统在搜索与救援场景中的弱点。