夏里宾

电话：(+86) 13738339739 | 邮箱：lbxia@stu.pku.edu.cn

教育背景

北京大学 计算机学院 网络安全专业 **2022.09 - 2025.06**

上海交通大学 电子信息与电器工程学院 信息安全专业 **2018.09 - 2022.06**

• **GPA**：3.90/4.30 **排名**：5/129 **学业奖项**：二等奖学金、学业进步奖学金、全国大学生物理竞赛上海市一等奖

研究方向

• **密码学技术**：安全多方计算（秘密分享、混淆电路、同态加密、不经意传输），零知识证明，群签名，环签名

• **密码学应用**：大模型安全，隐私保护机器学习，访问控制，去中心化身份，匿名凭证，领域特定语言

论文发表

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

Libin Xia, Xihan Zhang, Jiashuo Zhang, Ke Wang, Yue Li, Jianbo Gao, Zhi Guan, Zhong Chen.

The 40th ACM Annual Computer Security Applications Conference (ACSAC'24) (CCF B), 2024 (submitted)

提出了新颖的去中心化访问控制方案Heimdall，实现了公平访问和策略机密性。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时间从而实现公平访问。重构了混淆电路方案并在协议中整合零知识证明在恶意用户的模型下实现访问控制策略的机密性，同时保证用户身份的机密性。

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

Libin Xia, Jiashuo Zhang, Che Wang, Zezhong Tan, Jianbo Gao, Zhi Guan, Zhong Chen.

The 31st IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER'24) (CCF B), 2024.

设计了基于密码学任务的领域特定语言CryptLang，支持三种以太坊中最常用的加密类别：承诺、签名和摘要。同时设计了编译器CRYPTCODER能够自动将这些CryptLang语言转换为Solidity语言并部署在链上。

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

Libin Xia, Jiashuo Zhang, Xihan Zhang, Yue Li, Jianbo Gao, Zhi Guan, Zhong Chen.

The 5th IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS'23), 2023.

利用群签名算法设计了匿名且可追踪的身份凭证，利用零知识证明实现了身份属性的选择性披露和可组合性质。

实习经历

华为技术有限公司 2012实验室 数据与隐私保护实验室 （导师：周李京） **2024.7 - 2024.10**

主要研究方向为安全多方计算在隐私保护机器学习上的应用（包括大模型的隐私推断与训练）。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。设计了高效安全的分布式比较函数，实现了端到端的安全模型推断系统。

科研项目

国家重点研发计划 | 双层一体安全高性能区块链智能合约语言关键技术研究 **2022.11 - 2023.11**

• 项目任务：领域模型及智能合约领域特定语言族设计，智能合约代码合成与转译技术。

• 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；我设计了语言转译系统，实现从CryptLang到Solidity的自动化转译；我将CryptLang以模块的形式整合到BPMN中，给出了具体应用示范。

国家重点研发计划 | 非开源联盟链基础平台 **2023.11 - 2024.11**

• 项目任务：基于用户属性及场景的访问控制系统，研究基于秘密分享和零知识证明的密态数据计算技术

• 我利用秘密分享、混淆电路和零知识证明，设计了去中心化访问控制协议，实现了身份，数据和访问控制策略的隐私，并实现公平的访问控制。我利用秘密分享，静默可验证证明，批处理和小空间素描技术，设计了隐私聚合系统，实现了在恶意用户模型下的高效率低存储的隐私数据分析。

科学专利

基于CryptLang的隐私合约构建方法和代码生成系统

• 申请人：博雅正链（北京）科技有限公司，北京大学

• 发明人：夏里宾，张家硕，张锡涵，高健博，谢安明，关志，李青山，陈钟

技能水平

• **编程语言**：Python, Solidity, JavaScript, C++, Go, Rust, Circom, Zokrates.