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（混淆电路、秘密分享、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，去中心化访问控制，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)

• **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.

• **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.

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

Xihan Zhang, Jiashuo Zhang, Jianbo Gao, Libin Xia, Zhi Guan, Hao Hu, Zhong Chen.

Frontiers of Computer Science (FCS'24) (CCF B), 2024.

实习经历

博雅正链（北京）科技有限公司（导师公司） **2022.11 - 2024.6**

我会负责一些公司所承担的国家重点研发计划的项目，同时也负责与重庆分公司的业务人员进行对接。

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**

我负责大模型安全协议设计，包括利用秘密分享，同态加密，混淆电路，零知识证明等密码学技术实现针对恶意用户的大模型隐私推断，针对线性与非线性函数的安全运算加速，并尝试将安全算法集成在GPU中。我还调研了蚂蚁的可信计算框架隐语平台，包括SPU等隐私保护机器学习的计算模块。

科研项目

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

• 项目任务：面向联盟链的多维安全和隐私保护技术，基于用户属性及场景的访问控制系统。

• 我使用秘密分享、混淆电路和零知识证明方案，设计了基于去中心化身份的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。

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

• **英语水平**：CET6 545

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