

夏里宾

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

* **核心课程**：计算机系统安全、网络和信息安全等；

**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
* **核心课程**：网络和信息安全、数据结构、编译原理、操作系统等；
* **竞赛获奖：**美国大学生数学建模竞赛国际二等奖（H奖）,全国大学生物理竞赛上海市一等奖

# 研究兴趣

* **区块链上安全与隐私协议设计：**去中心化身份，匿名凭证，去中心化访问控制
* **应用密码学：**零知识证明，群签名，环签名，可验证秘密分享
* **软件工程：**领域特定语言

# 论文发表

**会议论文**

**• 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.

**期刊论文**

**• 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 - 2024.11

# 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。

# 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**

* 项目介绍：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。
* 我负责项目中的课题5：智能合约领域特定语言族(DSLs)及领域示范应用，设计了区块链上民生领域的DSL，设计了从DSL到solidity的转译编译器，测试分析了语言的具体应用场景，并进行BPMN的整合测试工作。

**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**

* 项目介绍：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。
* 我负责项目中的课题3：面向区块链的多层次多维度安全和隐私保护体系，使用公开可验证的秘密分享和非交互零知识证明方案，设计了基于细粒度策略的去中心化访问控制协议。

# 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

# 教学经历

**信息安全概论 助教** **2022.9-2023.6**

# 技能水平

* **英语水平：**CET6 545
* **编程语言：**Python, Solidity, JavaScript, C++, Go, Circom, Zokrates.