

沈博文

哈尔滨工业大学（深圳） | shenbowen@stu.hit.edu.cn | +86-13120460300 | 个人主页

教育背景

哈尔滨工业大学（深圳） 鹏城实验室联培，博士，计算机科学与技术	2024.09 – 至今
- 导师：蒋琳教授；研究方向：安全多方计算，隐私保护大模型	
北京航空航天大学，巴黎萨克雷大学，双硕士，电子信息	2021.09 – 2024.07
- 导师：郭华教授；研究方向：安全多方计算	
北京航空航天大学，学士，网络空间安全	2017.09 – 2021.07

论文专利

- Bowen Shen, Yuyue Chen, Peng Yang, Bin Zhang*, Xi Zhang, Zoe L. Jiang*. SecMoE: Communication-Efficient Secure MoE Inference via Select-Then Compute. (**AAAI 2026**)
- Chen Chen, Hua Guo*, Yapeng Wu, **Bowen Shen**, Mingyang Ding, Jianwei Liu. A Lightweight Authentication and Key Agreement Protocol for IoT-Enabled Smart Grid System. (**Sensors**)
- 专利“支持数据分区的双服务器轻量化可搜索加密方法及系统”，以及软件著作权；

奖学金与科研资助

- 2024年北京航空航天大学优秀毕业生
- 2022年国家公派留学基金资助一年
- 2022 2023年北京航空航天大学学业奖学金一等奖
- 2020年全国大学生信息安全竞赛作品赛国家二等奖
- 2020年北京航空航天大学学科竞赛奖学金一等奖

科研经历

哈工大-浦发银行金融网络空间安全联合创新中心项目	2024.02 – 2024.09
- 合作项目“现有FATE加密算法的安全漏洞研究”。旨在针对现有联邦学习FATE框架下算法的安全漏洞进行分析，针对安全性和效率问题提出面向FATE框架的隐私计算算法。	
- 设计并开发基于MPC和FHE的高效安全两方计算协议，代码验收并整合进波塞冬框架，申请发明专利1项。	
深圳重大-跨域隐私计算平台项目	2024.02 – 2025.12
- 深圳市纵向项目“基于密态协同计算的全过程跨域数据共享平台”。旨在解决安全多方计算难以在大规模密态数据协同计算中落地应用等问题，设计并实现低通信算法及应用。	
- 负责设计并实现10种隐私计算平台新型隐私保护机器学习训练方法，在数据量 50000×500 下典型模型训练时间 $\leq 3000s$ 。	
蚂蚁隐私计算专项科研项目	2022.10 – 2023.10
- 参与“基于SecureNN密态协议的研究和优化”，实现SecureNN的NN样例，并对接隐语原生框架，验证其通信和带宽消耗，以及其在部分算子下相比于ABY3的适用性。	
- 参与实现SecureNN的5个基本算子，针对卷积层、ReLU、网络结构、除法算子以及硬件加速方面进行MPC优化，实现既定算子下速度超过ABY3。	

技术技能

- 编程: Python, C++
工具: LaTeX, Git, Linux, Docker
语言: 中文（母语），英语雅思6.5；