王屿轩

男 · 汉族 · 2000-09 · 籍贯北京
18588297218@sjtu.edu.cn · /18801354216 ·
擅长领域：后量子密码学、硬件安全（侧信道分析及故障分析）、深度学习

教育背景

上海交通大学 (推免)，网络空间安全，学术型博士生 (硕博连读) **2022.9 – 至今**

导师谷大武教授 (长江学者，讲席教授，网安学院院长), 预计 2028 年 6 月毕业（**已满足毕业要求，毕业时间可与导师协商**），博士入学考试笔试面试均为专业第一，GPA 3.62/4.0

上海交通大学，信息安全，工学学士 **2018.9 – 2022.6**

25 门专业课获得 A 及以上成绩, 综合排名 22/130，获校级优秀学士学位论文提名

荣誉及获奖情况

所获奖学金情况

连续三年获得上海交通大学校一、二等学业奖学金 2019，2020，2021

连续四年上海交通大学研究生学业奖学金 2022，2023，2024，2025

中国网络空间安全协会网安专业资助计划（奖金伍万元） 2025

专业竞赛获奖情况

美国大学生数模竞赛 一等奖、全国大学生英语竞赛二等奖、全国大学生物理竞赛 二等奖 2019

本科生研究计划国家级项目获评 A+ 2020

全国大学生信息安全作品赛二等奖，互联网 + 大赛铜奖 2021，2022

代表论文及专利

研究方向: 后量子密码算法的侧信道分析及故障分析，深度学习技术在硬件安全中的应用

1. **Yuxuan Wang**, Jintong Yu, Shipei Qu, Xiaolin Zhang, *et al.* Mind the Faulty Keccak: A Practical Fault Injection Attack Scheme Apply to All Phases of ML-KEM and ML-DSA. *IEEE TIFS*, 2025. (信息安全顶刊，已发表) CCF-A
2. **Yuxuan Wang**, Jintong Yu, Yihan Nie, Yubo Zhao, *et al.* Neur-SASCA: High-Noise-Tolerant and Automated Single-Trace Attack against NTT. *IACR CHES*. 2026 (硬件安全顶会，已录用) CCF-B
3. **Yuxuan Wang**, Jintong Yu, Yihan Nie, Yubo Zhao, *et al.* Profiling-Device-Free SASCA Framework for ML-KEM. (*IEEE TIFS* 在投)
4. **Yuxuan Wang**, Jintong Yu, Pei Cao, Yubo Zhao, *et al.* CAPE: Cross-Block Deep Learning Framework for Non-profiled Side-Channel Analysis. (*ESORICS 2026* 在投)
5. Jintong Yu, **Yuxuan Wang**, Shipei Qu, Yubo Zhao, *et al.* End-to-End Non-profiled Side-Channel Analysis on Long Raw Traces. *ESORICS*, 2025. (已发表) CCF-B
6. Shipei Qu, **Yuxuan Wang**, Jintong Yu, Chi Zhang, *et al.* Trace copilot: Automatically locating cryptographic operations in side-channel traces by firmware binary instrumenting. *IACR CHES*, 2025. (硬件安全顶会，已发表) CCF-B
7. Jintong Yu, **Yuxuan Wang**, Zixin He, Yihan Nie, *et al.* Blind Leakage: Rethinking Deep Learning-based Non-Profiled Side-Channel Analysis (*IACR CHES 2026* 在投)
8. Jintong Yu, **Yuxuan Wang**, Pei Cao, Zixin He, *et al.* TAME: A Deep Learning-based Blind Side-Channel Analysis Framework. (*IACR CHES 2026* 在投)
9. Shipei Qu, **Yuxuan Wang**, Jintong Yu, Cheng Hong, *et al.* Find the Clasp of the Chain: Efficiently Locating Cryptographic Procedures in SoC Secure Boot by Semi-automated Side-Channel Analysis *ICICS*, 2025. (已发表) CCF-C
10. Yubo Zhao, Shipei Qu, **Yuxuan Wang**, Jintong Yu, *et al.* SpectroLoc: Cryptographic Operation Localization via Spectrogram Projection and Time-Series Analysis. *IACR CHES*. 2026 (硬件安全顶会，已录用) CCF-B
11. Xiaolin Zhang, Chenghao Chen, Kailun Qin, **Yuxuan Wang**, *et al.* Now Let's Make It Physical: Enabling Physically Trusted Certificate Issuance for Keyless Security in CAs. *IEEE TCAD*. 2026 (已录用) CCF-A
12. 申请中专利：一种针对后量子密码算法的故障分析方法；一种针对后量子密码算法的深度学习侧信道分析方法 第一发明人
13. 面向信息流的安全推荐系统, CN113609394A, 发明授权. 第三发明人

部分成果支撑上海市技术发明一等奖：面向密码模块的新型信息泄漏分析和防护技术研究 (第一完成人谷大武)

接后页

专业技能

- 熟悉 ML-KEM、ML-DSA 等后量子密码算法，侧信道分析及故障分析，密码学，深度学习等相关领域；具有丰富的侧信道分析及故障分析实战经验及神经网络训练经验。
- 可熟练运用 Python，C/C++（嵌入式开发）等编程语言，熟练使用 Claude Code、Codex 等大模型辅助编程工具，擅长快速学习新技术并搭建各类小型原型系统；
- 擅长项目协作管理与沟通协调，有较强的责任心。在实验室作为学生负责人主导完成多个横向、纵向项目；
- 写作功底扎实，有多类科技材料的写作经验（包括学术论文、发明专利、申报书、项目指南、技术报告等）；
- 英语读写能力较好，TOEFL 97 分, 研究生学术英语、学术写作课程均获得 A 等成绩；
- 有丰富的工作汇报经历与材料筹备经验；多次负责各类答辩路演、大会报告、项目评审的汇报素材制作，如 2024 年上海市科技发明奖答辩材料、多个国自然面上/联合基金的答辩材料、2025 中国信息和通信安全学术会议等；

项目与实践经历

- 独立完成华为项目 *针对基于格的后量子密码的能量侧信道攻击的防护方案*，*主导完成*国安某单位 USIM 卡黑盒分析项目（保密），作为 *核心骨干*参与解放军某部后量子硬件分析相关项目（保密）、中船某所侧信道分析相关项目（保密）、智巡商用密码检测中心 *密码检测引擎关键技术研究*第一、二期等，完成多款密码检测工具开发；
- 作为 *学生负责人* 主导申报并实施国家自然基金联合基金 *后量子密码实践安全性机理及分析方法*、面上基金 *密码模块的故障攻击：科学机理和实验验证*，参与申报、成果产出、进度汇报、答辩等全流程。作为 *核心骨干* 参与国家重点研发项目 *密码芯片信息泄漏深度分析与基于可靠防护的芯片研制*。
- 2025 年作为 *核心骨干* 参与筹建国家级密码检测机构 *上海浦东密码研究院*（已揭牌成立），参与制定研究院研究内容、职能规划、年度目标等，独立为研究院开发 *后量子密码故障分析软硬件平台*、*后量子密码侧信道分析平台*；
- 参与 NIST LWC 轻量级密码算法评测，研究 GIFT-COFB、Romulus 和 Ascon 算法的差分故障分析。

代表性经历详情

后量子密码算法 ML-KEM 和 ML-DSA 的故障分析方案设计 **2023 年 9 月 – 2024 年 12 月**

设计了首个适用于 ML-KEM 和 ML-DSA 所有加密流程的故障分析方案

- 以后量子密码中通用的哈希组件 Keccak 为目标，构建针对 ML-KEM 和 ML-DSA 的密钥恢复、签名伪造攻击方案；
- 在 5 款不同 ARM Cortex-M 架构的嵌入式设备上实现攻击实例（C，Python），并设计搭建软硬件分析平台；

后量子密码算法 ML-KEM 的深度学习单曲线侧信道分析 **2024 年 6 月 – 2025 年 9 月**

提出首个基于深度学习的针对 ML-KEM 的单曲线分析方案，分析能力达国际最优

- 设计多输出神经网络架构，并结合信念传播网络实现单曲线分析，提供 NTT 信念传播算法的快速实现；
- 在真实嵌入式设备高噪声、非对齐、跨设备分析的场景具有显著优势，快速实现使分析效率提升十倍以上；

后量子密码算法 ML-KEM 的跨运算侧信道分析 **2025 年 8 月 – 至今**

提出首个无需建模设备的软分析侧信道攻击（SASCA）方案，大幅增强针对 ML-KEM 的黑盒分析能力

- 基于 NTT 与 INTT 的相似性，使用无监督域适应（UDA）实现同设备跨运算建模，取消了 SASCA 的建模设备假设；
- 在真实的 ARM 架构嵌入式设备上给出开源分析框架（C，Python）并验证分析效果；

非建模跨运算侧信道分析框架设计 **2026 年 1 月 – 至今**

提出首个跨运算联合分析的非建模分析框架，攻击所需曲线数相比最先进方法减少 60% 以上

- 在基于深度学习的非建模侧信道分析中，基于迁移学习技术实现联合利用多运算泄露，提出多泄露聚合评分算法；
- 以多种回归/分类模型为基础，在真实的 ARM 架构嵌入式设备上给出开源分析框架（C，Python）；

NIST 国际标准轻量级密码算法候选算法实现的安全性评估 **2022 年 4 月 – 2022 年 8 月**

个人负责评估 GIFT-COFB、Romulus 和 Ascon 认证加密标准候选算法的抗故障分析能力

- 为三种 LWC 密码算法设计并实现差分故障分析理论方案；
- 评估结果为 Ascon 的 S 盒设计抗故障分析安全性最高，与 NIST 最终评选结果一致；

其他经历

- 参与设计国际首个端到端深度学习非建模侧信道分析方案 ConvWIN-MCR，参与方案设计与理论证明；
- 研究针对智能手机 DVFS 机制的故障注入分析（clkscrew），并形成适用于 nexus 6 手机的分析实例和开源代码；
- 参与研究基于 Transformer 架构的抗投毒攻击的鲁棒推荐系统；
- 实习经历：2022 年 6-8 月，中国人民银行软件开发中心，“金融电子云”开发；2022 年 8-9 月，灵伴智能，算法岗