王文浩

手机：(+86) 15210983075 · **邮箱：**wangwenhao@iie.ac.cn

中国科学院信息工程研究所 · 副研究员

个人网址：https://heartever.github.io

工作经历

中国科学院信息工程研究所，副研究员 2018 年 11 月 至今

- 信息安全国家重点实验室 → 网络空间安全防御全国重点实验室
- 主要研究方向为机密计算、系统安全、侧信道攻击
- 开设中国科学院大学研究生课程《安全芯片技术》(40 学时)

美国印第安纳大学，访问学者 2016 年 4 月 至 2018 年 8 月

- 合作导师：王晓峰教授，ACM SIGSAC 主席，IEEE 会士
- 由 NIH 项目资助，主要工作之一是协助组织隐私计算顶级赛事 iDASH 安全基因组分析竞赛，负责讨论和制定赛题、提供基线解决方案以及对参赛队伍提交方案的安全性、性能等各方面的评测

中国科学院信息工程研究所，助理研究员 2015 年 1 月 至 2018 年 10 月

- 信息安全国家重点实验室
- 主要研究方向为隐私计算、可信执行环境、侧信道攻击、硬件辅助系统安全、密码学

教育背景

中国科学院大学，信息安全，博士 2009 年 9 月 至 2015 年 1 月

- 导师：林东岱研究员

中国海洋大学，计算机科学与技术，本科 2005 年 9 月 至 2009 年 7 月

部分发表论文 (✉ 通信作者，__ 由我指导，[ ] 排名不分先后)

- *The Early Bird Catches the Leak: Unveiling Timing Side Channels in LLM Serving Systems*
  [Linke Song, Zixuan Pang], **Wenhao Wang**✉, Zihao Wang, XiaoFeng Wang, Hongbo Chen, Wei Song, Yier Jin, Dan Meng, Rui Hou
  IEEE Transactions on Information Forensics and Security (TIFS) (CCF-A)
- *CryptPEFT: Parameter-Efficient Fine-Tuning for Privacy-Preserving Neural Network Inference*
  Saisai Xia, **Wenhao Wang**✉, Zihao Wang✉, Yuhui Zhang, Yier Jin, Dan Meng, Rui Hou
  Network and Distributed System Security Symposium (NDSS) 2026 (CCF-A)
- *Multivariate Template Attack against NTT based Polynomial Multiplication of Dilithium*
  Haopeng Fan, Hailong Zhang✉, Yongjuan Wang✉, **Wenhao Wang**, Yanbei Zhu, Haojin Zhang, Qingjun Yuan
  IEEE Transactions on Information Forensics and Security (TIFS) (CCF-A)

- *Comet: Accelerating Private Inference for Large Language Model by Predicting Activation Sparsity*
  Guang Yan, Yuhui Zhang✉, Zimu Guo, Lutan Zhao, Xiaojun Chen, Chen Wang, **Wenhao Wang**, Dan Meng, Rui Hou✉
  2025 IEEE Symposium on Security and Privacy (S&P) (CCF-A)
- *The Road to Trust: Building Enclaves within Confidential VMs*
  Wenhao Wang, Linke Song, Benshan Mei, Shuang Liu, Shijun Zhao, Shoumeng Yan✉, XiaoFeng Wang, Dan Meng, Rui Hou✉
  Network and Distributed System Security Symposium (NDSS) 2025 (CCF-A)
- *Screening Least Square Technique assisted Multivariate Template Attack against the Random Polynomial Generation of Dilithium*
  Haopeng Fan, Hailong Zhang✉, Yongjuan Wang✉, **Wenhao Wang**, Yanbei Zhu, Haojin Zhang, Qingjun Yuan
  IEEE Transactions on Information Forensics and Security (TIFS) (CCF-A)
- *ThermalScope: A Practical Interrupt Side Channel Attack Based On Thermal Event Interrupts*
  Xin Zhang, Zhi Zhang, Qingni Shen, **Wenhao Wang**, Yansong Gao, Zhuoxi Yang, Zhonghai Wu
  The 61st Design Automation Conference (DAC 2024) (CCF-A)
- *Cache attacks on subkey calculation of Blowfish*
  Haopeng Fan,**Wenhao Wang**✉, Yongjuan Wang, Xiangbin Wang, Yang Gao
  Journal of Computer Security (JCS) (CCF-B)
- *PP-Stream: A Privacy-Preserving Neural Network Inference Service with Stream Processing*
  Qingxiu Liu, Qun Huang, Xiang Chen, Sa Wang, **Wenhao Wang**, Shujie Han, Patrick P. C. Lee
  40th IEEE International Conference on Data Engineering (ICDE 2024) (CCF-A)
- *Verifying Rust Implementation of Page Tables in a Software Enclave Hypervisor*
  Zhenyang Dai, Shuang Liu, Vilhelm Sjoberg✉, Xupeng Li, Yu Chen, **Wenhao Wang**, Yuekai Jia, Sean Noble Anderson, Laila Elbeheiry, Shubham Sondhi, Yu Zhang, Zhaozhong Ni, Shoumeng Yan✉, Ronghui Gu, Zhengyu He
  International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2024) (CCF-A)
- *Tossing in the Dark: Practical Bit-Flipping on Gray-box Deep Neural Networks for Runtime Trojan Injection*
  Zihao Wang, Di Tang✉, XiaoFeng Wang, Wei He, Zhaoyang Geng, **Wenhao Wang**✉
  USENIX Security 2024 (CCF-A)
- *SegScope: Probing Fine-grained Interrupts via Architectural Footprints*
  Xin Zhang, Zhi Zhang, Qingni Shen, **Wenhao Wang**, Yansong Gao, Zhuoxi Yang, Jiliang Zhang
  30th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024) (CCF-A)
- *The Danger of Minimum Exposures: Understanding Cross-App Information Leaks on iOS through Multi-Side-Channel Learning*
  [Zihao Wang, Jiale Guan], XiaoFeng Wang, **Wenhao Wang**, Luyi Xing, Fares Alharbi
  ACM Conference on Computer and Communications Security (ACM CCS 2023) (CCF-A)
- *WhistleBlower: A System-level Empirical Study on RowHammer*

[Wei He, Zhi Zhang], Yueqiang Cheng, **Wenhao Wang**✉, Wei Song, Yansong Gao, Qifei Zhang, Kang Li, Dongxi Liu, Surya Nepal
IEEE Transactions on Computers (TC) (CCF-A)

- *Implicit Hammer: Cross-Privilege-Boundary Rowhammer through Implicit Accesses*
[Zhi Zhang, Wei He], Yueqiang Cheng, **Wenhao Wang**, Yansong Gao✉, Dongxi Liu, Kang Li, Surya Nepal, Anmin Fu, Yi Zou
IEEE Transactions on Dependable and Secure Computing (TDSC) (CCF-A)
- *HyperEnclave: An Open and Cross-platform Trusted Execution Environment*
Yuekai Jia, Shuang Liu, **Wenhao Wang**✉, Yu Chen, Zhengde Zhai, Shoumeng Yan, Zhengyu He
2022 USENIX Annual Technical Conference (USENIX ATC) (CCF-A)
- *SoftTRR: Protect Page Tables Against RowHammer Attacks using Software-only Target Row Refresh*
[Zhi Zhang, Yueqiang Cheng], Minghua Wang, Wei He, **Wenhao Wang**✉, Nepal Surya, Yansong Gao, Kang Li, Zhe Wang, Chenggang Wu
2022 USENIX Annual Technical Conference (USENIX ATC) (CCF-A)
- *Trust Beyond Border: Lightweight, Verifiable User Isolation for Protecting In-Enclave Services*
Wenhao Wang, Weijie Liu, Hongbo Chen, XiaoFeng Wang, Hongliang Tian, Dongdai Lin
IEEE Transactions on Dependable and Secure Computing (TDSC) (CCF-A)
- *BitMine: An End-to-End Tool for Detecting Rowhammer Vulnerability*
[Zhi Zhang, Wei He], Yueqiang Cheng, **Wenhao Wang**, Yansong Gao✉, Minghua Wang, Kang Li, Surya Nepal, Yang Xiang
IEEE Transactions on Information Forensics & Security (TIFS) (CCF-A)
- *Practical and Efficient in-Enclave Verification of Privacy Compliance*
Weijie Liu, **Wenhao Wang**✉, Hongbo Chen, XiaoFeng Wang✉, Xiaozhu Meng, Yaosong Lu, Hongbo Chen, Xinyu Wang, Qingtao Shen, Kai Chen, Haixu Tang, Yi Chen, Luyi Xing
51st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021) (CCF-B)
- *Randomized Last-Level Caches Are Still Vulnerable to Cache Side-Channel Attacks! But We Can Fix It*
Wei Song, Boya Li, Zihan Xue, Zhenzhen Li, **Wenhao Wang**, Peng Liu
2021 IEEE Symposium on Security and Privacy (S&P 2021) (CCF-A)
- *Enabling Rack-scale Confidential Computing using Heterogeneous Trusted Execution Environment*
Jianping Zhu, Rui Hou✉, XiaoFeng Wang✉, **Wenhao Wang**, Jiangfeng Cao, Boyan Zhao, Zhongpu Wang, Yuhui Zhang, Jiameng Ying, Lixin Zhang, Dan Meng
2020 IEEE Symposium on Security and Privacy (S&P 2020) (CCF-A)
- *Bluethunder: A 2-level Directional Predictor Based Side-Channel Attack against SGX*
Tianlin Huo, Xiaoni Meng, **Wenhao Wang**✉, Chunliang Hao, Pei Zhao, Jian Zhai, Mingshu Li✉
IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES 2020) (CCF-B)
- *Beware of Your Screen: Anonymous Fingerprinting of Device Screens for Off-line Payment Protection*
Zhe Zhou, Di Tang, **Wenhao Wang**, XiaoFeng Wang, Zhou Li, Kehuan Zhang Annual Computer Security Applications Conference (ACSAC 2018) (CCF-B)

- *Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery*
  Meicheng Liu, Jingchun Yang, **Wenhao Wang**, Dongdai Lin
  37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2018) (CCF-A)
- Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races
  [Guoxing Chen, **Wenhao Wang**✉], Tianyu Chen, Sanchuan Chen, Yinqian Zhang, XiaoFeng Wang, Ten-Hwang Lai, Dongdai Lin
  2018 IEEE Symposium on Security and Privacy (S&P 2018) (CCF-A)
- *A community effort to protect genomic data sharing, collaboration and outsourcing*
  Shuang Wang, Xiaoqian Jiang, Haixu Tang, Xiaofeng Wang, Diyue Bu, Knox Carey, Stephanie OM Dyke, Dov Fox, Chao Jiang, Kristin Lauter, Bradley Malin, Heidi Sofia, Amalio Telenti, Lei Wang, **Wenhao Wang**, Lucila Ohno-Machado
  NPJ genomic medicine
- *iDASH secure genome analysis competition 2017*
  XiaoFeng Wang, Haixu Tang, Shuang Wang, Xiaoqian Jiang, **Wenhao Wang**, Diyue Bu, Lei Wang, Yicheng Jiang, Chenghong Wang
  BMC Medical Genomics 2018
- *Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX*
  Wenhao Wang, Guoxing Chen, Xiaorui Pan, Yinqian Zhang, XiaoFeng Wang, Vincent Bindschaedler, Haixu Tang, Carl A. Gunter
  2017 ACM Conference on Computer and Communications Security (CCS 2017) (CCF-A)

其它论文 (✉ 通信作者，__ 由我指导，[ ] 排名不分先后)

- *Learning from Proof-of-Concepts: Hybrid Fuzzing of Deep Learning Compilers and Libraries*
  Zizhuang Deng, Sanchuan Chen, Guozhu Meng, **Wenhao Wang**, Tong Liu, Xueqing Zhang, Yidi Kao, Kai Chen
  In submission
- *virtCCA: Virtualized Arm Confidential Compute Architecture with TrustZone*
  Xiangyi Xu, **Wenhao Wang**✉, Yongzheng Wu, Zhennan Min, Zixuan Pang, Yier Jin✉
  In submission
- *Understanding TEE Containers, Easy to Use? Hard to Trust*
  [Weijie Liu, Hongbo Chen], XiaoFeng Wang, Zhi Li, Danfeng Zhang, **Wenhao Wang**, Haixu Tang
  In submission
- *Toward Scalable Fully Homomorphic Encryption Through Light Trusted Computing Assistance*
  Wenhao Wang, Yichen Jiang, Qintao Shen, Weihao Huang, Hao Chen, Shuang Wang, XiaoFeng Wang, Haixu Tang, Kai Chen, Kristin Lauter, Dongdai Lin

专利

- *System for decentralized ownership and secure sharing of personalized health data*
  Shuang Wang, XiaoFeng Wang, Haixu Tang, **Wenhao Wang**, Ali Farahanchi, Hao Zheng
  US Patent 11,003,791

学术服务

- 会议大会主席：Inscrypt 2022
- 会议程序委员会委员：CCS (2019)，GenoPri (2020, 2021)，ACNS (2023) 等
- 期刊论文评阅专家：IEEE TDSC，IEEE Security & Privacy，IEEE TC，ACM Transactions on Privacy and Security，CyberSecurity，SCN，JNCA，信息安全学报等
- 会议论文评阅专家: CCS (2018, 2020), NDSS (2017, 2018, 2021), S&P (2017, 2020, 2021), Usenix Security (2017, 2018, 2021), HPCA (2019), ESORICS (2018, 2020), Asiacrypt (2020), AsiaCCS (2017, 2018, 2019), RECOMB (2019) 等

学术奖励

- 2018 年度 ACM 中国新星奖提名（全国范围内共 3 名）
- 2018 年度 ACM 中国 SIGSAC 分会新星奖（分会范围内共 2 名）
- 2017 年度中国科学院信息工程研究所“青年之星”

项目资助

- 中国科学院战略性先导科技专项课题, 机密计算基础理论, 课题负责人, 2038.1 万元(2023.12–2028.11)
- 华为公司产学研合作项目，基于下一代异构计算的机密容器与设备直通技术研究，负责人，153.7 万元（2023.12 – 2025.12）
- 国家自然科学基金面上项目，基于虚拟机级可信执行环境的安全容器架构研究，负责人，54 万元（2023.1 – 2026.12）
- 国家自然科学基金重大研究计划重点支持项目，深度学习隐私保护计算新型体系框架与模型，课题负责人（项目下设 4 个课题），约 300 万元（2023.1 – 2026.12）
- CCF-华为胡杨林基金可信计算专项，面向虚拟机级可信执行环境的安全容器架构研究，负责人，30 万元（2022.9 – 2023.8）
- 蚂蚁产学研合作项目，可信执行环境技术融合统一架构，负责人，30 万元（2022.9 – 2023.8）
- 科技部重点研发计划，基于 mRNA 免疫的可信任网络寻址与路由控制技术，课题骨干，428 万元（2020.11 – 2024.10）
- 信息工程研究所攀登计划，后量子密码算法实现中的安全问题研究，负责人，30 万元（2021.1 – 2022.12）
- 国家自然科学基金青年基金项目，英特尔软件防护扩展抗侧信道泄漏安全性研究，负责人，30 万元（2019.1 – 2021.12）
- 信息工程研究所青年之星，负责人，10 万元（2018.1 – 2020.12）

部分学术报告

- “看懂可信执行环境硬件设计-浅析 TEE 的内存加密和完整性保护机制”，隐私计算联盟安全研讨会，2022 年 3 月，线上
- “从软件角度防范侧信道攻击”，2020 年国际测试委员会智能计算机与芯片联合大会，2020 年，线上
- “英特尔 SGX 侧信道安全研究”，南京航空航天大学线上报告，2020 年 3 月，线上
- “英特尔 SGX 侧信道安全研究”，BenchCouncil2019 国际芯片大会，2019 年 12 月，北京
- “基于硬件可信执行环境技术的隐私计算”，第四届中国数据安全与隐私保护大会，2019 年 10 月，广西桂林
- “可信执行环境技术前沿”，中国科学院大学科学前沿讲座，2019 年 10 月，北京
- “基于二级方向预测器的侧信道攻击”，2019 年，河南郑州
- “机密计算”，南开大学，2019 年 7 月，天津
- “可信执行环境中的侧信道风险”，中国图灵大会，2019 年 4 月，四川成都