

PERSONAL INFORMATION

Name: Guowen Xu
Date of Birth: 5 June, 1991
E-Mail: guowen.xu@foxmail.com
Phone: +852 97054118
Homepages: <https://guowen-xu.github.io/>
Address: City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, Hong Kong



EDUCATION BACKGROUND

- Ph.D. of Cyberspace Security 2015/09-2020/12
(Supervisor: Prof. **Hongwei Li: IEEE Fellow**)
School of Computer Science and Engineering
University of Electronic Science and Technology of China (UESTC)
- Visiting Ph.D. in Cyberspace Security 2019/08-2020/08
(Supervisor: Prof. **Robert H. Deng: IEEE Fellow**)
School of Information of Systems
Singapore Management University
- Bachelor of Information and Computing Science 2010/09-2014/06
School of Mathematical and Physical Science
Anhui Jianzhu University (AHJZU)

PROFESSIONAL EXPERIENCE

- Research Fellow 2021/03-2023/05
School of Computer Science and Engineering
Nanyang Technological University, Singapore
- Postdoc (Supervisor: Prof. **Yuguang Fang: IEEE Fellow**) 2023/05-2024/05
Department of Computer Science
City University of Hong Kong
- Professor 2024/05-Present
School of Computer Science and Engineering, UESTC

RESEARCH INTERESTS

Applied Cryptography; Computer Security; AI Security and Privacy.

AWARDS AND HONORS

- **2023 Stanford World's Top 2% Scientists**
- **2023 IEEE BigDataSecurity Best Paper Award**
- 2022-2024 Distinguished Reviewer of ACM Transactions on the Web
- 2022 ECCV Online Registration Waiver Award, Committee of ECCV
- **2021 Wu Wenjun First Prize of Artificial Intelligence Science and Technology Progress**
- 2021 Outstanding Graduate Student of University of Electronic Science and Technology of China
- 2021 Outstanding Graduate Student in Sichuan Province
- 2021 IEEE INFOCOM Student Conference Award
- **2020 IEEE ICPADS Best Paper Award**
- 2020 National Scholarship of Graduate Student (MOE of PRC, Top 1%)
- 2020 First-class Scholarship of Graduate Student (UESTC, Top 1%)
- 2019 SCF Best Student Paper Award (Sichuan Province Computer Federation)

- 2019 National Scholarship of Graduate Student (MOE of PRC, Top 1%)
- 2019 First-class Scholarship of Graduate Student (UESTC, Rank: Top 1%)
- 2018 Network Security Scholarship of China Internet Development Foundation
- 2018 National Scholarship of Graduate Student (MOE of PRC, Top 1%)
- 2018 First-class Scholarship of Graduate Student (UESTC, Top 1%)
- 2018 First-class Scholarship of Shenzhen Huiding Technology Co.,Ltd (Top 1%)
- 2018-2020 Excellent Student Award (UESTC)
- 2018-2020 Excellent Graduate Student (UESTC)
- 2016 Excellence award of National Cipher Technology Competition

SELECTED PUBLICATIONS (CCF A papers: **30**, Google Citations: **2814**; 2024/01/30)

- [1] **[S&P 2024]** Xingshuo Han, Yutong Wu, Qingjie Zhang, Yuan Zhou, Yuan Xu, Han Qiu, **Guowen Xu**, and Tianwei Zhang. Backdooring Multimodal Learning[C]. in *IEEE Symposium on Security and Privacy*, 2024. (CCF A)
- [2] **[INFOCOM 2024]** Xinyuan Qian, Hongwei Li, **Guowen Xu**, Haoyong Wang, Tianwei Zhang, Xianhao Chen, Yuguang Fang. Privacy-Preserving Data Evaluation via Functional Encryption, Revisited. in *Proceedings of IEEE International Conference on Computer Communications*, 2024. (CCF A)
- [3] **[ICRA 2024]** Yuang Zhang, Haonan An, Zhengru Fang, **Guowen Xu**, Yuan Zhou, Xianhao Chen, Yuguang Fang. SmartCooper: Vehicle Collaborative Perception under Adaptive Fusion and Judger Mechanism. *IEEE International Conference on Robotics and Automation*, 2024. (CCF B)
- [4] **[TDSC 2023]** **Guowen Xu**, Xingshuo Han, Tianwei Zhang, Shengmin Xu, Jianting Ning, Xinyi Huang, Hongwei Li, Robert H.Deng. SIMC 2.0: Improved Secure ML Inference Against Malicious Clients [J]. *IEEE Transactions on Dependable and Secure Computing*, 2023. (CCF A).
- [5] **[TDSC 2023]** **Guowen Xu**, Xingshuo Han, Gelei Deng, Tianwei Zhang, Shengmin Xu, Jianting Ning, Anjia Yang, Hongwei Li. VerifyML: Obliviously Checking Model Fairness Resilient to Malicious Model Holder [J]. *IEEE Transactions on Dependable and Secure Computing*, 2023. (CCF A)
- [6] **[TIFS 2023]** **Guowen Xu**, Shengmin Xu, Jinhua Ma, Jianting Ning, and Xinyi Huang. An Adaptively Secure and Efficient Data Sharing System for Dynamic User Groups in Cloud [J]. *IEEE Transactions on Information Forensics and Security*, 2023. (CCF A)
- [7] **[TIFS 2023]** Jianfei Sun, **Guowen Xu***(Corresponding Author), Tianwei Zhang, Xuehuan Yang, Mamoun Alazab, Robert H. Deng. Privacy-aware and Security-enhanced Efficient Matchmaking Encryption [J]. *IEEE Transactions on Information Forensics and Security*, 2023, to appear. (CCF A)
- [8] **[TKDE 2023]** Zhuoran Ma, Jianfeng Ma, Yinbin Miao, **Guowen Xu**, Yang Liu, Ximeng Liu, Robert H. Deng. FLGAN: GAN-Based Unbiased Federated Learning under Non-IID Settings[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2023. (CCF A)
- [9] **[ICML 2023]** Haoxiao Chen, Hongwei Li, Meng Hao, Kangjie Chen, **Guowen Xu**, Tianwei Zhang, Xilin Zhang [C]. GuardHFL: Privacy Guardian for Heterogeneous Federated Learning. in *International Conference on Machine Learning*, 2023. (CCF A)
- [10] **[ICLR 2023]** Guanlin Li, **Guowen Xu***(Corresponding Author), Shangwei Guo, Han Qiu, Jiwei Li, Tianwei Zhang. Extracting Robust Models with Uncertain Examples[C]. in *International Conference on Learning Representations*. 2023.

- [11] [ICLR 2023] Kangjie Chen, Xiaoxuan Lou, Guowen Xu, Jiwei Li, Tianwei Zhang. Clean-image Backdoor: Attacking Multi-label Models with Poisoned Labels Only[C]. in *International Conference on Learning Representations*, 2023. (Notable-top-5%)
- [12] [TDSC 2023] Wenbo Jiang, Hongwei Li, Guowen Xu, Tianwei Zhang, Rongxing Lu. A Comprehensive Defense Framework against Model Extraction Attacks [J]. *IEEE Transactions on Dependable and Secure Computing*, 2023. (CCF A)
- [13] [CVPR 2023] Wenbo Jiang, Hongwei Li, Guowen Xu, Tianwei Zhang. Color Backdoor: A Robust Poisoning Attack in Color Space [C]. in *Proceedings of IEEE / CVF Computer Vision and Pattern Recognition Conference*, 2023. (CCF A)
- [14] [INFOCOM 2023] Dongyun Xue, Haomiao Yang, Mengyu Ge, Jingwei Li, Guowen Xu, Hongwei Li. Fast Generation-Based Gradient Leakage Attacks against Highly Compressed Gradients [C]. in *Proceedings of IEEE International Conference on Computer Communications*, 2023. (CCF A)
- [15] [TSC 2023] Shengmin Xu, Xingshuo Han, Guowen Xu, Jianting Ning, Xinyi Huang, Robert H. Deng. An Adaptive Secure and Practical Data Sharing System with Verifiable Outsourced Decryption [J]. *IEEE Transactions on Services Computing*, 2023, to appear. (CCF A)
- [16] [TCSVT 2023] Guowen Xu, Guanlin Li, Shangwei Guo, Tianwei Zhang, Hongwei Li. Secure Decentralized Image Classification with Multiparty Homomorphic Encryption[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2023. (CCF B)
- [17] [CCS 2022] Gelei Deng, Guowen Xu*(Corresponding Author), Yuan Zhou, Tianwei Zhang, Yang Liu. On the (In) Security of Secure ROS2[C]. in *Proceedings of ACM Conference on Computer and Communications Security*, 2022. (CCF A)
- [18] [TDSC 2022] Guowen Xu, Xingshuo Han, Shengmin Xu, Tianwei Zhang, Hongwei Li, Xinyi Huang, Robert H Deng. Hercules: Boosting the Performance of Privacy-preserving Federated Learning[J], *IEEE Transactions on Dependable and Secure Computing*, 2022. (CCF A)
- [19] [TIFS 2022] Jianfei Sun, Guowen Xu*(Corresponding Author), Xuehuan Yang, Tianwei Zhang, Mamoun Alazab, Robert H. Deng. Verifiable, Fair and Privacy-preserving Broadcast Authorization for Flexible Data Sharing in Clouds [J]. *IEEE Transactions on Information Forensics and Security*. 2022. (CCF A)
- [20] [TIFS 2022] Jianfei Sun, Guowen Xu*(Corresponding Author), Tianwei Zhang, Mamoun Alazab, Robert H. Deng. A Practical Fog-based Privacy-preserving Online Car-hailing Service System [J]. *IEEE Transactions on Information Forensics and Security*, 2022. (CCF A)
- [21] [ECCV 2022] Guanlin Li, Guowen Xu*(Corresponding Author), Han Qiu, Ruan He, Jiwei Li, Tianwei Zhang. Improving Adversarial Robustness of 3D Point Cloud Classification Models[C]. in *Proceedings of European Conference on Computer Vision*. 2022. (CCF B)
- [22] [TITS 2022] Jianfei Sun, Guowen Xu* (Corresponding Author) Tianwei Zhang, Xiaochun Cheng, Xingshuo Han, MingJian Tang. Secure Data Sharing with Flexible Cross-domain Authorization in Autonomous Vehicle Systems[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022. (CCF B)
- [23] [TIFS 2022] Hanxiao Chen, Hongwei Li, Yingzhe Wang, Meng Hao, Guowen Xu, Tianwei Zhang. PriVDT: An Efficient Two-Party Cryptographic Framework for Vertical Decision Trees [J]. *IEEE Transactions on Information Forensics and Security*, 2022. (CCF A)
- [24] [TDSC 2022] Wenbo Jiang, Tianwei Zhang, Han Qiu, Hongwei Li, Guowen Xu. Incremental Learning, Incremental Backdoor Threats[J]. *IEEE Transactions on Dependable and Secure Computing*, 2022. (CCF A)

- [25] [NeurIPS 2022] Meng Hao, Hongwei Li, Hanxiao Chen, Pengzhi Xing, Guowen Xu, Tianwei Zhang. Iron: Private Inference on Transformers [C]. in *Proceedings of Thirty-Sixth Conference on Neural Information Processing Systems*. 2022. (CCF A)
- [26] [MM 2022] Xingshuo Han, Guowen Xu, Yuan Zhou, Xuehuan Yang, Jiwei Li, Tianwei Zhang. Physical Backdoor Attacks to Lane Detection Systems in Autonomous Driving [C]. in *Proceedings of ACM International Conference on Multimedia*. 2022. (CCF A)
- [27] [TSC] Jingwei Wang, Xinchun Yin, Jianting Ning, Shengmin Xu, Guowen Xu, and Xinyi Huang. Secure Updatable Storage Access Control System for EHRs in the Cloud [J]. *IEEE Transactions on Services Computing*, 2022, to appear. (CCF A)
- [28] [INFOCOM 2021] Haoran Yuan, Xiaofeng Chen, Guowen Xu*(Corresponding Author), Jianting Ning, Joseph Liu, Robert H Deng. Efficient and Verifiable Proof of Replication with Fast Fault Localization[C]. in *Proceedings of IEEE International Conference on Computer Communications*, 2021. (CCF A)
- [29] [TCC 2021] Jianfei Sun, Guowen Xu*(Corresponding Author), Tianwei Zhang, Hu Xiong, Hongwei Li, Robert H Deng. Share your data carefree: An efficient, scalable and privacy-preserving data sharing service in cloud computing[J]. *IEEE Transactions on Cloud Computing*, 2021. (JCR-Q1)
- [30] [TDSC 2021] Shengmin Xu, Jianting Ning, Xinyi Huang, Yingjiu Li, Guowen Xu. Untouchable Once Revoking: A Practical and Secure Dynamic EHR Sharing System via Cloud[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021. (CCF A)
- [31] [TIFS 2021] Xiaoyuan Liu, Hongwei Li, Guowen Xu, Zongqi Chen, Xiaoming Huang, and Rongxing Lu. Privacy-Enhanced Federated Learning against Poisoning Adversaries [J]. *IEEE Transactions on Information Forensics and Security*, 2021. (CCF A)
- [32] [TDSC 2021] Shengmin Xu, Jianting Ning, Yingjiu Li, Yinghui Zhang, Guowen Xu, Xinyi Huang, Robert H. Deng. A Secure EMR Sharing System with Tamper Resistance and Expressive Access Control[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021. (CCF A)
- [33] [ESORICS 2021] Shengmin Xu, Jianting Ning, Jinhua Ma, Guowen Xu, Jiaming Yuan, Robert Deng. Revocable Policy-Based Chameleon Hash [C], in *Proceedings of European Symposium on Research in Computer Security*, 2021. (CCF B)
- [34] [ACSAC 2021] Meng Hao, Hongwei Li, Guowen Xu, Hanxiao Chen, Tianwei Zhang. Efficient, Private and Robust Federated Learning[C]. in *Proceeding of Annual Computer Security Applications Conference*, online, 2021. (CCF B)
- [35] [TDSC 2020] Guowen Xu, Hongwei Li, Yun Zhang, Shengmin Xu, Jianting Ning, Robert H. Deng. Privacy-preserving Federated Deep Learning with Irregular Users[J]. *IEEE Transactions on Dependable and Secure Computing*, 2020. (CCF A)
- [36] [ASIACCS 2020] Guowen Xu, Hongwei Li, Shengmin Xu, Hao Ren, Kan Yang, Yinghui Zhang, Jianfei Sun, Robert H. Deng. Catch You If You Deceive Me: Verifiable and Privacy-aware Truth Discovery in Crowd Sensing Systems[C]. in *Proceedings of ACM ASIA Conference on Computer and Communications Security*, Taipei, Taiwan, China, 2020. (CCF C)
- [37] [ACSAC 2020] Guowen Xu, Hongwei Li, Hao Ren, Jianfei Sun, Shengmin Xu, Jianting Ning, Haomiao Yang, Kan Yang, Robert H. Deng. Secure and Verifiable Inference in Deep Neural Networks[C]. in *Proceeding of Annual Computer Security Applications Conference*, 2020. (CCF B)
- [38] [TCC 2020] Guowen Xu, Hongwei Li, Hao Ren, Xiaodong Lin, Xuemin (Sherman) Shen. DNA Similarity Search with Access Control over Encrypted Cloud Data[J]. *IEEE Transactions on Cloud Computing*, 2019. (JCR-Q1)

- [39] [ICPADS 2020] **Guowen Xu**, Hongwei Li, Yuan Zhang, Xiaodong Lin, Robert H Deng, Xuemin (Sherman) Shen. A Deep Learning Framework Supporting Model Ownership Protection and Traitor Tracing[C]. in *Proceedings of IEEE International Conference on Parallel and Distributed Systems*, 2020. (**Best Paper Award**)
- [40] [TDSC 2020] Shengmin Xu, Jianting Ning, Yingjiu Li, Yinghui zhang, **Guowen Xu**, Xinyi Huang, Robert H Deng. Match in My Way: Fine-Grained Bilateral Access Control for Secure Cloud-Fog Computing[J]. *IEEE Transactions on Dependable and Secure Computing*, 2020. (**CCF A**)
- [41] [TIFS 2019] **Guowen Xu**, Hongwei Li, Sen Liu, Kan Yang, Xiaodong Lin. VerifyNet: Secure and Verifiable Federated Learning[J]. *IEEE Transactions on Information Forensics and Security*, 2019. (**CCF A**)
- [42] [TVT 2019] **Guowen Xu**, Hongwei Li, Sen Liu, Mi Wen, Rongxing Lu. Efficient and Privacy-preserving Truth Discovery in Mobile Crowd Sensing Systems[J]. *IEEE Transactions on Vehicular Technology*, 2019. (**JCR-Q1**)
- [43] [IEEE Commun Mag 2019] **Guowen Xu**, Hongwei Li, Hao Ren, Kan Yang, Robert H. Deng. Data Privacy and Security in Deep Learning: Attacks, Solutions and Opportunities[J]. *IEEE Communications Magazine*, 2019. (**JCR-Q1**)
- [44] [TIFS 2018] **Guowen Xu**, Hongwei Li, Yuanshun Dai, Kan Yang, Xiaodong Lin. Enabling Efficient and Geometric Range Query with Access Control over Encrypted Spatial Data[J]. *IEEE Transactions on Information Forensics and Security*, 2018. (**CCF A**)
- [45] [CCS 2018] **Guowen Xu**, Hongwei Li, Rongxing Lu. Poster: Practical and Privacy-Aware Truth Discovery in Mobile Crowd Sensing Systems[C]. in *Proceedings of ACM Conference on Computer and Communications Security*, Toronto, Canada. 2018 (Poster).
- [46] [Comput Secur 2017] **Guowen Xu**, Hongwei Li, Chen Tan, Dongxiao Liu, Yuanshun Dai, Kan Yang. Achieving Efficient and Privacy-Preserving Truth Discovery in Crowd Sensing Systems[J]. *Computers & Security*, 2017. (**CCF B**)

PROJECT EXPERIENCES

- [2017.7-2020.6] Research on Heterogeneous Identity Alliance and Basic Scientific Issues of Supervision (National Key Research and Development Program of China), Amount: **¥15.9 million**.
- [2018.1-2021.12] Research on Searchable Encryption Technology Oriented to Practical Application (National Natural Science Foundation of China), Amount: **¥860,000**.
- [2020.1-2022.12] Research on Data Security and Privacy Issues in Edge Computing (Sichuan Youth Science and Technology Innovation Team Foundation), Amount: **¥1.2 million**.
- [2021.1-2025.12] Research on Security and Privacy Issues in Internet of Things Applications Based on Edge Computing (National Natural Science Foundation of China), Amount: **¥2.6 million**.
- [2022.1-2024.12] A Systematic Study about the Integrity Threats and Protection of Sensory Data in Autonomous Vehicles (NTU-Desay-SV), Amount: **S\$700K**.
- [2022.6-2025.06] A Framework for Intellectual Property Protection of Deep Learning Applications (MoE AcRF Tier2, Singapore), Amount: **S\$350K**.

TEACHING EXPERIENCES

- [**Teaching Assistant**] – School of Computer Science and Engineering (UESTC), Mar 2018 - Aug 2018
 - Worked as a Teaching Assistant (TA) for the Algorithm Design and Analysis Course.
 - Held recitations and solve students' questions during the course of study.
- [**Teaching Assistant**] – School of Computer Science and Engineering (UESTC), Sep 2017 - Jan 2018
 - Worked as a Teaching Assistant (TA) for the Network and System Attack Technology Course.

- Held recitations and solve students' questions during the course of study.

ACADEMIC TALKS

- “CryptMDB: A Practical Encrypted MongoDB over Big Data”, IEEE ICC 2017, Paris, France.
- “EFRS: Enabling Efficient and Fine-grained Range Search on Encrypted Spatial Data”, IEEE ICC 2018, Kansas, USA.
- “Enabling Efficient and Fine-grained DNA Similarity Search with Access Control over Encrypted Cloud Data”, WASA 2018, Tianjing, China.
- “Privacy-enhanced Deep Packet Inspection at Outsourced Middlebox”, WCSP 2018, Hangzhou, China
- “A Deep Learning Framework Supporting Model Ownership Protection and Traitor Tracing”, ICPADS 2020, Hong Kong, China.
- “Secure and Verifiable Inference in Deep Neural Networks”, ACSAC 2020, Austin, Texas, USA.

ACADEMIC ACTIVITIES

- Editorial Board:
 - Associate Editor of International Journal of Information Security and Privacy (CCF C), 2024-present
 - Academic Editor of IET Information Security (CCF C), 2023-present
 - Distinguished Reviewer Board for ACM Transactions on the Web (CCF B), 2022-present
 - Lead Guest Editor of IET Information Security (CCF C), 2023-2024
- Publicity Chair
 - 2018 International Workshop on Smart Sensing and Computing (IWSSC)
- Technical Committee:
 - 2024 Area Chair of International Conference on Machine Learning (ICML)
 - 2024 IEEE International Conference on Communications (ICC)
 - 2023 The ACM Web Conference
 - 2023-2024 Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI)
 - 2022-2024 Distinguished Review Board for ACM Transactions on the Web
 - 2022 International Conference on Knowledge Science, Engineering and Management (KSEM)
 - 2018 International Workshop on Smart Sensing and Computing (IWSSC)
- Session Chair: The 13th International Conference on Wireless Algorithms, Systems, and Applications
- Reviewer:
 - IEEE Transactions on Information Forensics and Security (TIFS)
 - IEEE Transactions on Dependable and Secure Computing (TDSC)
 - IEEE Transactions on Mobile Computing (TMC)
 - IEEE Transactions on Network and Service Management (TNSM)
 - IEEE Transactions on Intelligent Transportation Systems (TITS)
 - IEEE Transactions on Knowledge and Data Engineering (TKDE)
 - IEEE Transactions on Vehicular Technology (TVT)
 - IEEE Transactions on Services Computing (TSC)
 - IEEE Transactions on Neural Networks and Learning Systems (TNNLS)
 - IEEE Transactions on Circuits and Systems for Video Technology (TCSTV)
 - IEEE Internet of Things Journal (IoT-J)
 - IEEE Transactions on Reliability (TR)

- ACM Transactions on Sensor Networks (TOSN)
- ACM Transactions on Web(TWEB)
- IEEE/ACM Transactions on Networking (ToN)
- Peer-to-Peer Networking and Applications (PPNA)
- Thirty-sixth Conference on Neural Information Processing Systems (NeurIPS 2022)
- The 39th International Conference on Machine Learning (ICML 2022)
- IEEE / CVF Computer Vision and Pattern Recognition Conference (CVPR 2022, 2023)
- IEEE International Conference on Communications (ICC, 2018, 2019)
- IEEE Global Communications Conference (GLOBECOM, 2018, 2019, 2020)
- IEEE/CIC International Conference on Communications in China (ICCC 2015)
- Future Generation Computer Systems
- IEEE NETWORK
- Computers & Security
- Information Sciences
- Information Fusion