个人信息

姓名：徐国文

出生日期: 19910605
E-Mail**:** guowen.xu@ntu.edu.sg
个人主页：https://guowen-xu.github.io/
地址: Nanyang Technological University, 50 Nanyang Ave, 639798

教育背景

- 博士　网络空间安全　　电子科技大学计算机科学与工程学院　　2017-2020
- 硕士　计算机技术　　电子科技大学计算机学院（硕博连读）　2015-2017
- 本科　信息与计算科学　安徽建筑大学数理学院　　2010-2014

海外经历

- 联合培养博士　网络空间安全　　新加坡管理大学　　2019.08-2020.08
- 博士后 (Research Fellow)　　新加坡南洋理工大学　　2021.03-至今

研究方向

应用密码学，包括大数据与云计算安全隐私技术、可信AI技术以及深度学习安全与隐私技术.

获得奖励

- 2021 年吴文俊人工智能技术科技进步一等奖
- 2021 年电子科技大学优秀博士学位论文奖
- 2021 年 IEEE INFOCOM Student Travel Grant
- 2021 年四川省优秀毕业生
- 2021 年电子科技大学优秀毕业生
- 2020 IEEE ICPADS 最佳论文奖
- 2019 年四川省计算机学会优秀学生论文奖（全省仅四篇）
- 2018 年中国互联网发展基金会网络安全专项奖学金（全校仅三人）
- 2020 年博士研究生国家奖学金 （综合成绩排名 3/200）
- 2019 年博士研究生国家奖学金 （综合成绩排名 3/200）
- 2018 年博士研究生国家奖学金 （综合成绩排名 1/200）
- 2020 研究生学业一等奖学金（综合成绩排名 2/200）
- 2019 研究生学业一等奖学金（综合成绩排名 1/200）
- 2019 研究生学业一等奖学金（综合成绩排名 1/200）
- 2018 深圳汇顶科技一等奖学金（综合成绩排名 1/200）
- 2020 电子科技大学卓越学生奖
- 2019 电子科技大学卓越学生奖
- 2018 电子科技大学卓越学生奖
- 2020 电子科技大学优秀研究生
- 2019 电子科技大学优秀研究生
- 2018 电子科技大学优秀研究生
- 2016 全国密码技术竞赛优胜奖
- 2012 全国大学生数学建模竞赛一等奖（安徽赛区）

代表性论文　　(谷歌学术引用：1016 次；H 指数：13)

[1] [**TDSC 2022**] 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*, vol.19, no.2, pp.1364-1381, 2022**. (CCF A 类期刊**)

[2] [**TITS 2022**] Jianfei Sun, Guowen Xu*(**通讯作者**), Tianwei Zhang, Xiaochun Cheng, Xingshuo Han, MingJian Tang. Secure Data Sharing with Flexible Cross-domain Authorization in Autonomous Vehicle Systems. *IEEE Transactions on Intelligent Transportation Systems*, 2022, DOI: 10.1109/TITS.2022.3157309. (中科院 **JCR** 一区期刊)

[3] [**INFOCOM 2021**] Haoran Yuan, Xiaofeng Chen, **Guowen Xu***(**通讯作者**), 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*, Vancouver BC Canada, pp.1-9, 202. (**CCF A 类会议**)

[4] [**TCC 2021**] Jianfei Sun, Guowen Xu*(**通讯作者**), 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. *IEEE Transactions on Cloud Computing*, 2021, DOI: 10.1109/TCC.2021.3117998. (中科院 **JCR** 一区期刊)

[5] [**TIFS 2020**] Guowen Xu, Hongwei Li, Sen Liu, Kan Yang, Xiaodong Lin. VerifyNet: Secure and Verifiable Federated Learning[J]. *IEEE Transactions on Information Forensics and Security*, vol.15, pp.911-926. 2020. (**CCF A 类期刊；ESI 高被引论文**)

[6] [**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*, Austin, Texas, USA, 2020, 1-15. (信息安全领域著名会议)

[7] [**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, China, 2020. pp.1-15. (信息安全领域著名会议)

[8] [**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*, 2020. DOI: 10.1109/TCC.2020.2968893. (中科院 **JCR** 一区期刊；**IEEE Trans.**系列期刊)

[9] [**ICPADS 2020**] Guowen Xu, Hongwei Li, Yuan Zhang, Xiaodong Lin, Robert H Deng, Xuemin Shen. A Deep Learning Framework Supporting Model Ownership Protection and Traitor Tracing[C]. in *Proceedings of IEEE International Conference on Parallel and Distributed Systems*, Hong Kong, China, 2020. pp.1-9. (最佳论文奖)

[10] [**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*, vol.57, no.11, pp.116-122, 2019. (中科院 **JCR** 一区期刊)

[11] [**TIFS 2019**] 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, vol.14, no.4, pp.870-885, 2019. (**CCF A 类期刊**; **四川省计算机学会优秀学生论文奖**； **ESI 高被引论文**)

[12] [**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*, vol.68, no.4, pp.3854-3865, 2019. (**中科院 JCR 二区期刊**；**IEEE Trans.系列期刊**)

[13] [**CCS 2018**] **Guowen Xu**, Hongwei Li, Rongxing Lu. Practical and Privacy-Aware Truth Discovery in Mobile Crowd Sensing Systems[C]. in *Proceedings of ACM Conference on Computer and Communications Security*, Toronto. 2018, pp.2132-2134. (**Poster**) (**信息安全领域顶级会议**)

[14] [**Comput Secur 2017**] Guowen Xu, Hongwei Li, Chen Tan, Dongxiao Liu, Kan Yang. Achieving Efficient and Privacy-Preserving Truth Discovery in Crowd Sensing Systems[J]. *Computers & Security*, 2017, vol.69, pp.114 -126. (**中科院 JCR 二区期刊**；**CCF B 类期刊**)

[15] [**TII 2022**] Haoxiao Chen, Hongwei Li, Guishan Dong, Meng Hao, Guowen Xu, Xiaoming Huang, Zhe Liu. Practical Membership Inference Attack Against Collaborative Inference in Industrial IoT[J]. *IEEE Transactions on Industrial Informatics*, vol.18, no.1, pp.477-487, 2022. （**中科院 JCR 一区期刊**；**IEEE Trans.系列期刊**）

[16] [**TDSC 2022**] 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*,vol.19, pp.1064-1077,2022. （**CCF A 类期刊**）

[17] [**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,DOI: 10.1109/TDSC.2021.3106393. (**CCF A 类期刊**)

[18] [**TIFS 2021**] Xiaoyuan Liu, Hongwei Li, Guowen Xu, Zongqi Chen, Xiaoming Huang, and Rongxing Lu. 2021. Privacy-Enhanced Federated Learning against Poisoning Adversaries [J]. *IEEE Transactions on Information Forensics and Security*, vol.16, pp.4574-4588, 2021. (**CCF A 类期刊**)

[19] [**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, DOI: 10.1109/TDSC.2021.3126532. (**CCF A 类期刊**)

[20] [**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*, Virtual, 2021. (**信息安全领域著名会议**)

[21] [**ACSAC 2021**] Meng Hao, Hongwei Li, Guowen Xu, Hanxiao Chen, Tianwei Zhang. Efficient, Private and Robust Federated Learning. in *Proceeding of Annual Computer Security Applications Conference*, online, 2021, 1-15(**信息安全领域著名会议**)

[22] [**TII 2021**] Meng Hao, Hongwei Li, Xizhao Luo, Guowen Xu, Haomiao Yang and Sen Liu. Efficient and Privacy-enhanced Federated Learning for Industrial Artificial Intelligence[J]. *IEEE Transactions on Industrial Informatics*, vol.16, no.10, pp.6532-6542, 2020.（**中科院 JCR 一区期刊**；**ESI 高被引论文**）

[23] [**TCC 2021**] Guiqiang Hu, Hongwei Li, Guowen Xu, Xinqiang Ma. Enabling Simultaneous Content Regulation and Privacy Protection for Cloud Storage Image[J]. *IEEE Transactions on Cloud Computing*, 2021. DOI: 10.1109/TCC.2021.3081564. (**中科院 JCR 一区期刊；IEEE Trans.系列期刊**)

[24] [**TCSVT 2021**] Shangwei Guo, Tianwei Zhang, Guowen Xu, Han Yu, Tao Xiang, Yang Liu. Topology-aware Differential Privacy for Decentralized Image Classification[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2021, DOI:10.1109/TCSVT.2021.3105723. (**中科院 JCR 一区期刊；IEEE Trans.系列期刊**)

[25] [**IoT-J 2021**] Jianfei Sun, Dajiang Chen, Ning Zhang, Guowen Xu, Mingjian Tang, Xuyun Nie, Mingsheng Cao. A Privacy-aware and Traceable Fine-grained Data Delivery System in Cloud-assisted Healthcare IIoT. [J]. *IEEE Internet of things journal*, vol.8, no.12, pp.10034-10046, 2021. （**中科院 JCR 一区期刊**）

[26] [**IoT-J 2021**] Yiran Li, Hongwei Li, Guowen Xu, Xiaoming Huang, Rongxing Lu. Efficient Privacy-Preserving Federated Learning with Unreliable Users [J]. *IEEE Internet of things journal*, 2021, DOI: 10.1109/JIOT.2021.3130115. （**中科院 JCR 一区期刊**）

[27] [**TCC 2020**] Hao Ren, Hongwei Li, Dongxiao Liu, Guowen Xu，Nan Cheng, Sherman Shen. Privacy-preserving Efficient Verifiable Deep Packet Inspection for Cloud-assisted Middlebox[J]. *IEEE Transactions on Cloud Computing*. 2020. DOI: 10.1109/TCC.2020.2991167. （**中科院 JCR 一区期刊；IEEE Trans.系列期刊**）

[28] [**TCC 2020**] Hao Ren, Hongwei Li, Dongxiao Liu, Guowen Xu, Xuemin Shen. Enabling Secure and Versatile Packet Inspection with Probable Cause Privacy for Outsourced Middlebox[J]. *IEEE Transactions on Cloud Computing*, 2020. DOI: 10.1109/TCC.2021.3059026. (**中科院 JCR 一区期刊；IEEE Trans.系列期刊**)

[29] [**IoT-J 2020**] Yiran Li, Hongwei Li, Guowen Xu, Tao Xiang, Xiaoming Huang, Rongxing Lu. Towards Secure and Privacy-Preserving Distributed Deep Learning in Fog-Cloud Computing[J]. *IEEE Internet of things journal*, vol.7, no.12, pp.11460-11472, 2020. （**中科院 JCR 一区期刊**）

[30] [**IoT-J 2020**] Xiaoyuan Liu, Hongwei Li, Guowen Xu, Sen Liu, Zhe Liu, Rongxing Lu. PADL: Privacy-aware and Asynchronous Deep Learning for IoT Applications[J]. *IEEE Internet of things journal*, vol.7, no.8, pp.6955-6969, 2020. （**中科院 JCR 一区期刊**）

[31] **[Inf Sci 2020]** Shengmin Xu, Jiaming Yuan, Guowen Xu, Yingjiu Li, Ximeng Liu, Yinghui Zhang, Zoubin Ying. Efficient Ciphertext-Policy Attribute-Based Encryption with Blackbox Traceability[J]. ***Information Sciences***, vol.538, pp.19-38, 2020 （**中科院 JCR 一区期刊**）

[32] [**Sci. China Inf. Sci 2020**] Yinghui Zhang, Tiantian Zhang, Shengmin Xu, Guowen Xu, Dong Zheng. Revocable and cetificateless public auditing for cloud storage[J]. *SCIENCE CHINA Information Sciences*. 2020, vol.63, no.10, pp. 1-3. （**中科院 JCR 二区期刊**）

[33] **[FGCS 2019]** Wenbo Jiang, Hongwei Li, Guowen Xu, Mi Wen, Guishan Dong, and Xiaodong Lin. PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI[J]. *Future Generation Computer Systems*，2019，vol. 96, pp. 185-195. （**中科院 JCR 一区期刊**）

[34] [**ICC 2018**] Guowen Xu, Hongwei Li, Yuanshun Dai, Xiaodong Lin. EFRS: Enabling Efficient and Fine-grained Range Search on Encrypted Spatial Data[C]. in *Proceedings of IEEE International Conference on Communications*, 2018，Kansas, USA ,pp.1-6. (通信领域旗舰会议)

[35] **[ICC 2017**] Guowen Xu, Yan Ren, Hongwei Li, Dongxiao Liu, Yuanshun Dai, Kan Yang. CryptMDB: A Practical Encrypted MongoDB over Big Data[C]. in *Proceedings of IEEE International Conference on Communications*, Paris, France, 2017. pp.1-6. (通信领域旗舰会议)

[36] [**BigSecurity 2018**] Guowen Xu, Hongwei Li, Wenlei Wang, Yue Chen, Haomiao Yang, Yanzhi Ren. Towards Practical Personalized Recommendation with Multilevel Differential Privacy Controls[C]. in *Proceedings of International Workshop on Security and Privacy in Big Data*, Honolulu, HI, USA. pp.796-801, 2018.

[37] [**GLOBECOM 2016**] Guowen Xu, Hongwei Li, Dongxiao Liu, Hao Ren, Yuanshun Dai, Xiaohui Liang. Towards Efficient Privacy-Preserving Truth Discovery in Crowd Sensing Systems[C]. in *Proceedings of IEEE Global Communications Conference*, Washington, D.C, USA, 2016. pp.1-6.（通信领域旗舰会议)

已完成论文（Manuscripts）

[1] Privacy-preserving Decentralized Deep Learning with Multiparty Homomorphic Encryption 第一作者

[2] A Secure Fingerprinting Framework for Distributed Image Classification 第一作者

[3] SIMC 2.0: Improved Secure Inference Resilient to Malicious Clients 第一作者

[4] Hercules: Boosting the Performance of Privacy-preserving Federated Neural Network Learning 第一作者

[5] A Practical Fog-based Privacy-preserving Online Car-hailing Service System. 通讯作者

[6] Aligning with a Gaussian Disturibution Makes Your Model Robust. 通讯作者

[7] ShiftNAS: Towards Automatic Generation of Advanced Mulitplication-Less Neural Networks 通讯作者

[8] Fingerprinting Generative Adversarial Networks. 通讯作者

[9] Improving Adversarial Robustness of 3D Point Cloud Classification Models. 通讯作者

[10] Backdoor Attacks against Complex Systems, Not Just Individual Models. 通讯作者

[11] On the (In)Security of Secure ROS2. 通讯作者

[12] DPSEV: Differential Privacy against Fingerprinting Attacks on Secure Virtual Machines. 通讯作者

申请/授权专利

[1] 云环境下实现密文空间数据的访问控制和范围查询方法，已授权，CN201810692703.3

[2] 在移动群智感知系统中实现高效隐私保护的真值发现方法，已授权，CN201811322088.3

[3] 中毒样本生成方法、装置、设备及计算机可读存储介质，已授权，CN202010024362.X

[4] 数据隐私保护方法、装置及计算机可读存储介质，已授权，CN202010029622.2

[5] 在深度学习系统中基于数字指纹的验证与追踪方法，已受理，CN202011443755.0

[6] 自适性保护隐私的联邦深度学习的方法，已受理，CN201910563455.7

[7] 一种实现高效相似性查询和访问控制的基因数据脱敏方法，已受理，CN201910387357.2

[8] 在区块链 PKI 下支持瘦客户端的隐私保护身份认证方法，已受理， CN201810519096.0

[9] 一种机器学习逆过程中生成最优训练集的方法，已受理，CN201910250513.0

[10] 一种基于隐私保护的分布式深度学习方法，已受理，CN202010342081.9

[11] 面向非规则用户的保护隐私的联邦深度学习方法,已受理，CN202010360559.0

[12] 在移动群智感知系统中可验证的隐私保护方法,已受理，CN202010447473.1

[13] 在移动群智感知系统中可验证的、具有隐私意识的真相发现的方法,已受理，CN202010842682.6

[14] 在不规则用户中保留隐私的联邦学习的方法,已受理，CN202010262316.3

[15] 非关系型数据库加密系统 v1.0, 2018SR488991 （软著；已授权）

学术报告

- "CryptMDB: A Practical Encrypted MongoDB over Big Data", IEEE International Conference on Communications, 2017, 法国巴黎
- "EFRS: Enabling Efficient and Fine-grained Range Search on Encrypted Spatial Data", IEEE International Conference on Communications, 2018, 美国堪萨斯
- "Enabling Efficient and Fine-grained DNA Similarity Search with Access Control over Encrypted Cloud Data", International Conference on Algorithms, Systems, and Applications of Wireless Networks 2018, 中国天津
- "Practical and Privacy-Aware Truth Discovery in Mobile Crowd Sensing Systems", ACM Conference on Computer and Communications Security, 2018, 加拿大多伦多
- "Catch You If You Deceive Me: Verifiable and Privacy-aware Truth Discovery in Crowd Sensing Systems", ACM ASIA Conference on Computer and Communications Security, 2020, 中国台湾
- "Privacy-enhanced Deep Packet Inspection at Outsourced Middlebox", International Conference on
- Wireless Communications and Signal Processing, 2018, 中国杭州
- "A Deep Learning Framework Supporting Model Ownership Protection and Traitor Tracing", IEEE International Conference on Parallel and Distributed Systems, 2020, 中国香港
- "Secure and Verifiable Inference in Deep Neural Networks", Proceeding of Annual Computer Security Applications Conference, 2020, 美国奥斯汀

学术兼职

- 审稿人:
  - IEEE Transactions on Information Forensics and Security
  - IEEE Transactions on Dependable and Secure Computing
  - IEEE Transactions on Network and Service Management
  - IEEE Transactions on Mobile Computing
  - IEEE Transactions on Intelligent Transportation Systems
  - IEEE Transactions on Neural Networks and Learning Systems
  - IEEE Transactions on Knowledge and Data Engineering
  - IEEE Transactions on Network Science and Engineering
  - IEEE Transactions on Vehicular Technology

- IEEE Transactions on Services Computing
- IEEE Internet of Things Journal
- Peer-to-Peer Networking and Applications
- 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)
- IEEE NETWORK

➢ 程序委员会委员:

- 2018 International Workshop on Smart Sensing and Computing
- 2022 International Conference on Knowledge Science, Engineering and Management (KSEM)

➢ 分会主席：The 13th International Conference on Wireless Algorithms, Systems, and Applications