Runhua Xu

Professor, School of Computer Science and Engineering, Beihang University, China
runhua@buaa.edu.cn ⋄ runhua.xu@outlook.com ⋄ runhua.me

Areas of Specialization/Interest

Privacy Enhancing Technologies ∘ Federated Learning ∘ Privacy-Preserving Machine Learning
Blockchain and Smart Contract ∘ Applied Cryptography ∘ Access Control
Trustworthy, Transparent and Collaborative Cryptographic Infrastructure

Professional Experience

2024-PR. Professor, Beihang University, Beijing, China.
2023 AP, Beihang University, Beijing, China.
2020-2022 Research Staff Member, IBM Research - Almaden Research Center, San Jose, U.S.
2019 Research Intern, IBM Research - Almaden Research Center, San Jose, U.S.
2017-2020 Teaching Fellow/Assistant, University of Pittsburgh, Pittsburgh, U.S.
2015-2020 Research Assistant, University of Pittsburgh and LERSAIS, Pittsburgh, U.S.

Education

2015-2020 **Ph.D.** in Information Security, University of Pittsburgh, Pittsburgh, U.S.
- Advisor: **IEEE Fellow Prof. James Joshi**

2011-2014 **M.S.** in Computer Science, Beihang University, Beijing, China.
- Advisor: **Prof. Bo Lang**

2007-2011 **B.E.** in Software Engineering, Northwestern Polytechnical University, Xi'an, China.

Grants and Projects

2024-2026 Privacy-Enhancing Technologies for Federated Learning, NSF of China (Grant.62302022). PI.
2023-2025 Privacy-Enhanced Federated Learning, Beihang University Youth Talent Program. PI.
2020-2022 Enterprise Federated Learning Framework, IBM Research (Grant 3352/4774). Participant.
2019-2020 Secure and Private Federated Learning Framework for Enterprises, IBM Research (Grant 968). Participant.
2016-2018 SAC-PA: Towards Security Assured Cyberinfrastructure in Pennsylvania, NSF-CICI (No.1642117). Participant.
2016-2018 A Curriculum for Security Assured Health Informatics, NSF-DGE Award (No.1438809). Participant.

Publications

Journal Articles

[J8] Chao Li, **Runhua Xu**, Balaji Palanisamy, Li Duan, Meng Shen, Jiqiang Liu and Wei Wang. Blockchain Takeovers in Web 3.0: An Empirical Study on the TRON-Steem Incident. *ACM Transactions on the Web (ACM TWEB)*. ACM 2024. (accepted.)

[J7] **Runhua Xu**, Bo Li, Chao Li, James Joshi, Shuai Ma and Jianxin Li. TAPFed: Threshold Secure Aggregation for Privacy-Preserving Federated Learning. *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*. IEEE 2024.

[J6] **Runhua Xu**, Chao Li, and James Joshi. Blockchain-based Transparency Framework for Privacy Preserving Third-party Services. *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*. IEEE 2022.

[J5] **Runhua Xu**, James Joshi and Chao Li. NN-EMD: Efficiently Training Neural Networks using Encrypted Multi-sourced Datasets. *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*. IEEE 2021.

[J4] **Runhua Xu** and James B.D. Joshi. Trustworthy and Transparent Third Party Authority. *ACM Transactions on Internet Technology (ACM TOIT)*. ACM 2020.

[J3] **Runhua Xu**, James B.D. Joshi and Prashant Krishnamurthy. An Integrated Privacy Preserving Attribute Based Access Control Framework Supporting Secure Deduplication. *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*. IEEE 2019.

[J2] **Runhua Xu**, and Bo Lang. A CP-ABE scheme with hidden policy and its application in cloud computing. *International Journal of Cloud Computing*. Springer 2015.

[J1] Bo Lang, **Runhua Xu**, and Yawei Duan. Self-contained Data Protection Scheme Based on CP-ABE. *E-Business and Telecommunications, Communications in Computer and Information Science*. Springer 2014.

Conference and Workshop Articles

[C18] Chao Li, Balaji Palanisamy, **Runhua Xu**, Li Duan, Jiqiang Liu and Wei Wang. How hard is takeover in dpos blockchains? understanding the security of coin-based voting governance. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, pp. 150-164. 2023. (**Distinguished Paper Award**).

[C17] Chao Li, **Runhua Xu** and Li Duan. Liquid democracy in DPoS blockchains. In Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure, pp. 25-33. 2023.

[C16] Chao Li, **Runhua Xu** and Li Duan. Characterizing Coin-Based Voting Governance in DPoS Blockchains. In Proceedings of the International AAAI Conference on Web and Social Media, vol. 17, pp. 1148-1152. 2023.

[C15] Chao Li, Balaji Palanisamy, **Runhua Xu**, and Li Duan. Cross-Consensus Measurement of Individual-level Decentralization in Blockchains. In 2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), pp. 45-50. IEEE, 2023.

[C14] **Runhua Xu**, Nathalie Baracaldo, Yi Zhou, Ali Anwar, Heiko Ludwig. DeTrust-FL: Efficient Privacy-Preserving Federated Learning in Decentralized Trust Setting. *In 2022 IEEE International Conference on Cloud Computing (IEEE CLOUD 2022).* Hybrid event in Barcelona, Spain, IEEE 2022. (**Best Paper Award**).

[C13] **Runhua Xu**, Nathalie Baracaldo, Yi Zhou, Ali Anwar, James Joshi, Heiko Ludwig. FedV: Privacy-Preserving Federated Learning over Vertically Partitioned Data. *In the 14th ACM Workshop on Artificial Intelligence and Security (ACM AISec'21), co-located with ACM CCS'21.* November 15, 2021, Virtual Event. ACM 2021.

[C12] Chao Li, Balaji Palanisamy, **Runhua Xu**, Jinlai Xu and Jingzhe Wang. SteemOps: Extracting and Analyzing Key Operations in Steemit Blockchain-based Social Media Platform. *In 11th ACM Conference on Data and Application Security and Privacy (ACM CODASPY'21)*, Virtual Event, USA. ACM 2021.

[C11] **Runhua Xu** and James B.D. Joshi. Revisiting Secure Computation Using Functional Encryption: A Comprehensive Study. *In The 2ed IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS'20)*, IEEE 2020.

[C10] Chao Li, Balaji Palanisamy, **Runhua Xu**, Jian Wang, Jiqiang Liu. NF-Crowd: Nearly-free Blockchain-based Crowdsourcing. *In 2020 International Symposium on Reliable Distributed Systems (SRDS'20)*, Shanghai, China. IEEE 2020.

[C9] **Runhua Xu**, Nathalie Baracaldo, Yi Zhou, Ali Anwar and Heiko Ludwig. HybridAlpha: An Efficient Approach for Privacy-Preserving Federated Learning. *In 12th ACM Workshop on Artificial Intelligence and Security (ACM AISec'19), co-located with ACM CCS'19*, November 15, 2019, London, United Kingdom. ACM 2019.

[C8] **Runhua Xu**, James B.D. Joshi and Chao Li. CryptoNN : Training Neural Networks over Encrypted Data. *In The 39th IEEE International Conference on Distributed Computing Systems (ICDCS'19)*, Dallas, USA. IEEE 2019.

[C7] Chao Li, Balaji Palanisamy, and **Runhua Xu**. Scalable and Privacy-preserving Design of On/Off-chain Smart Contracts. *In The First International Workshop on Blockchain and Data Management (BlockDM'19)*, Macau SAR, China, IEEE 2019.

[C6] **Runhua Xu**, Balaji Palanisamy and James Joshi. QueryGuard: Privacy-preserving Latency-aware Query Optimization for Edge Computing. *In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'18)*, New York, USA. 2018.

[C5] **Runhua Xu**, James B.D. Joshi, Prashant Krishnamurthy and David Tipper. Insider Threat Mitigation in Attribute based Encryption. *In 9th Annual National Cyber Summit (Research Track)*, Von Braun Center, Huntsville, AL, USA. 2017.

[C4] **Runhua Xu** and James B.D. Joshi. Enabling Attribute Based Encryption as an Internet Service. *In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC'16)*, Pittsburgh, USA. IEEE, 2016.

[C3] **Runhua Xu** and James B.D. Joshi. An Integrated Privacy Preserving Attribute Based Access Control Framework. *In 2016 IEEE 9th International Conference on Cloud Computing (CLOUD'16)*, San Francisco, USA. IEEE, 2016.

[C2] **Runhua Xu**, Yang Wang, and Bo Lang. A Tree-Based CP-ABE Scheme with Hidden Policy Supporting Secure Data Sharing in Cloud Computing. *In Advanced Cloud and Big Data (CBD'13), 2013 International Conference on,* Nanjing, China. IEEE, 2013.

[C1] Bo Lang, **Runhua Xu**, and Yawei Duan. Extending the ciphertext-policy attribute based encryption scheme for supporting flexible access control. *In Security and Cryptography (SECRYPT'13), 2013 International Conference on,* Reykjavik, Iceland. IEEE, 2013.

Articles in Preprint and Under Peer Review

[X1] **Runhua Xu**, Nathalie Baracaldo and James B.D. Joshi. Privacy-Preserving Machine Learning: Methods, Challenges and Directions. (preprint arXiv:2108.04417)

[X2] **Runhua Xu**, Shiqi Gao, Chao Li, James Joshi, and Jianxin Li. Dual Defense: Enhancing Privacy and Mitigating Poisoning Attacks in Federated Learning. (under peer review)

Book Chapter

[B2] **Runhua Xu**, Nathalie Baracaldo, Yi Zhou, Annie Abay and Ali Anwar. Privacy-Preserving Vertical Federated Learning. *Federated Learning: A Comprehensive Overview of Methods and Applications.* Ludwig, H., Baracaldo, N. (eds). Springer, Cham. pp.281–312. 2022.

[B1] Nathalie Baracaldo and **Runhua Xu**. Protecting Against Data Leakage in FederatedLearning: What approach should you choose? *Federated Learning: A Comprehensive Overview of Methods and Applications.* Ludwig, H., Baracaldo, N. (eds). Springer, Cham. pp.281–312. 2022.

Patent

[P6] Eyal Kushnir, Hayim Shaul, Omri Soceanu, Ehud Aharoni, Nathalie Baracaldo Angel, **Runhua Xu**, Heiko H Ludwig. Secure reordering using tensor of indicators. *Patent Application 17/895,711*, filed March 14, 2024.

[P5] **Runhua Xu**, Nathalie Baracaldo Angel, Hayim Shaul, Omri Soceanu. Private vertical federated learning. *Patent Application 17/875,987*, filed Feberary 1, 2024.

[P4] Ali Anwar, Yi Zhou, Nathalie Baracaldo Angel, **Runhua Xu**, Yuya Jeremy Ong, Annie K Abay, Heiko H Ludwig, Gegi Thomas, Jayaram Kallapalayam Radhakrishnan, Laura Wynter. Grouped aggregation in federated learning. *U.S. Patent Application 17/807,871*, filed Dec 21, 2023.

[P3] Shiqiang Wang, Timothy John Castiglia, Nathalie Baracaldo Angel, Stacy Elizabeth Patterson, **Runhua Xu**, Yi Zhou. Vertical federated learning with secure aggregation. *Patent Application 17/838,445*, filed December 14, 2023.

[P2] Nathalie Baracaldo, **Runhua Xu**, Yi Zhou, Ali Anwar, and Heiko Ludwig. Efficient private vertical federated learning. *U.S. Patent 11,588,621*, filed Feb 21, 2023. **[Granted]**

[P1] **Runhua Xu,** Nathalie Baracaldo, Yi Zhou, Ali Anwar, and Heiko Ludwig. Privacy-preserving federated learning. *U.S. Patent Application 16/682927*, filed May 13, 2021.

Academia Service and Activities

Conference Organization and Service

- *Proceeding/Publicity/Workshop/Tutorial Chair*, IEEE International Conference on Collaboration and Internet Computing (IEEE CIC 2020, 2021, 2022, 2023, 2024)
- *Proceeding/Publicity/Workshop/Tutorial Chair*, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS 2020, 2021, 2022, 2023, 2024)
- *Proceeding/Publicity/Workshop/Tutorial Chair*, IEEE International Conference on Cognitive Machine Intelligence (IEEE CogMI 2020, 2021, 2022, 2023, 2024)
- *PC Member*, IEEE International Conference on Big Data (IEEE BigData 2021, 2022, 2023, 2024)
- *Organization Chair*, The 2023 International Workshop on Privacy-Preserving Machine Learning.

Journal Reviewer

- IEEE Transactions on Information Forensics and Security(TIFS)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Services Computing (TSC)
- IEEE Transactions on Mobile Computing (TMC)
- IEEE Transactions on Parallel and Distributed Systems (TPDS)
- IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)
- IEEE Transactions on Computers (TC)
- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE Transactions on Industrial Informatics (TII)
- IEEE Transactions on Neural Networks and Learning Systems(TNNLS)
- IEEE Transactions on Cloud Computing (TCC)
- IEEE Transactions on Big Data (TBD)
- IEEE Transactions on Green Communications and Networking (TGCN)
- IEEE Journal on Selected Areas in Communications (JSAC)
- IEEE Transactions on Emerging Topics in Computing (TETC)
- IEEE Transactions on Network Science and Engineering (TNSE)
- IEEE Transactions on Artificial Intelligence (TAI)
- IEEE Transactions on Consumer Electronics (TCE)
- IEEE Security and Privacy
- IEEE Intelligent Systems
- ACM Transactions on Internet Technology (TOIT)
- ACM Transactions on Knowledge Discovery fromData (TKDD)
- Computers & Security (COSE)
- Security and Communication Networks (SCN)
- Springer Neural Processing Letters (NEPL)
- Journal of Computer Science and Technology (JCST)
- International Journal of Cooperative Information Systems (IJCIS)
- Information Sciences (IS)
- Frontiers of Computer Science (FCS)
- Journal of Computer Science and Technology (JISA)
- Information Processing Letters (IPL)
- Expert Systems with Applications (ESWA)

Teaching Experience

Instructor/Teaching Fellow

- *Research Seminar: Privacy-Preserving Machine Learning.* School of Computer Science and Engineering, Beihang University. (2024 Spring)
- *Advanced Object-Oriented Programming.* School of Computer Science and Engineering, Beihang University. (2023 Fall)
- INFSCI 2150/TELCOM 2810 *Information Security and Privacy (including Online).* School of Computing and Information, University of Pittsburgh. (2016 Summer, 2016 Fall, 2017 Summer, 2017 Fall, 2018 Summer)

Teaching Assistant

- INSCI 2955 *Special Topics on Security Assured Health Informatics.* School of Computing and Information, University of Pittsburgh. (2018 Fall)
- INFSCI 2620 *Developing Secure Systems.* School of Computing and Information, University of Pittsburgh. (2017 Fall, 2018 Fall)
- INFSCI 1074 *Computer Security.* School of Computing and Information, University of Pittsburgh. (2017 Fall, 2019 Fall)
- INFSCI 2621/TELCOM 2813 *Security Management and Computer Forensics.* School of Computing and Information, University of Pittsburgh. (2017 Spring, 2018 Spring)
- INFSCI 1017 *Implementation of Information System.* School of Computing and Information, University of Pittsburgh. (2017 Spring)
- INFSCI 2150/TELCOM 2810 *Information Security and Privacy.* School of Computing and Information, University of Pittsburgh. (2016 Spring, 2016 Fall)

Honors and Awards

2023 ACM CCS 2023 Distinguished Paper Award.
2023 China Blockchain Excellent Paper Award.
2022 IEEE CLOUD 2022 Best Paper Award.
2019-2023 Excellent Service Award, IEEE CIC, IEEE TPS, IEEE CogMI 2019-2023.
2018 Ranked 6th, Cyber Defense Competition, Department of Energy, United States.
2018 Excellent Service Award, IEEE CIC 2018.
2016 Service Award, IEEE CIC 2016.
2016 Student Travel Award, IEEE Cloud 2016.
2012-2013 The Scholarship of Graduate, Beihang University. (2 times)
2008-2011 The Scholarship of Undergraduate, Northwestern Polytechnical University.(3 times)