Runhua Xu

Ph.D., Research Staff Member
AI Security and Privacy Solutions, AI Platforms, IBM Research - Almaden

EMAIL: runhua@ibm.com | runhua.xu@pitt.edu | runhua.xu@outlook.com
URL: IBM Research | Personal
ADDRESS: 650 Harry Rd, San Jose, CA *95120* U.S.

Areas of Specialization

secure computing • privacy-preserving collaborative machine learning
applied cryptography • blockchain and public ledger • access control
security and privacy issues in edge/cloud computing

Education

2015-2020 PH.D. in Information Security, University of Pittsburgh, Pittsburgh, U.S.

2011-2014 M.S. in Computer Science, Beihang University [1], Beijing, China.

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

Publications & Talks

Journal Articles

2020 **Runhua Xu** and James B.D. Joshi. "Trustworthy and Transparent Third Party Authority." ACM Transactions on Internet Technology. ACM 2020.

2019 **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 2019.

Conference articles

2020 **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 2020), IEEE 2020.

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

2019 **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(AISec'19), November 15, 2019, London, United Kingdom. ACM 2019.

2019 **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 2019), Dallas, USA. IEEE 2019.

2019 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 2019), Macau SAR, China, IEEE 2019.

2018 **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)*, New York, USA. 2018.

2017 **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.

2016 **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*, Pittsburgh, USA. pp. 417-426. IEEE, 2016.

[1] Beihang University, previously known as Beijing University of Aeronautics and Astronautics

2016 **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*, San Francisco, USA. pp. 68-76. IEEE, 2016.

2015 **Runhua Xu**, and Bo Lang. "A CP-ABE scheme with hidden policy and its application in cloud computing." *International Journal of Cloud Computing, Advanced Cloud and Big Data.* vol. 4, no. 4, pp. 279-298. 2015.

2014 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* pp. 306-321. 2014.

2013 **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), 2013 International Conference on,* Nanjing, China. pp. 51-57. IEEE, 2013.

2013 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), 2013 International Conference on,* Reykjavik, Iceland. pp. 1-11. IEEE, 2013.

2012 **Runhua Xu** and Bo Lang. "Survey on security model of authenticated key exchange protocols." *The 9th Graduate Students Academic Forum of Beihang University.* pp. 434-442. 2012. (in Chinese)

Academia Service & Activities

Journal Reviewer (including sub-reviews)

IEEE Transactions on Information Forensics and Security(TIFS),
IEEE Transactions on Services Computing (TSC),
IEEE Access,
ACM Transactions on Internet Technology (TOIT).

Conference Reviewer (including external reviews)

IEEE International Conference on Distributed Computing Systems (ICDCS 2017, 2019)
IEEE International Conference on Big Data (BigData 2016, 2019)
IEEE International Conference on Collaboration and Internet Computing (CIC 2016, 2017, 2018, 2019)
IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS 2019)
IEEE International Conference on Services Computing (SCC 2017)
IEEE International Conference on Smart Computing (SMARTCOMP 2019)
IEEE International Conference on Data Science in Cyberspace (DSC 2019);
ACM Conference on Data and Application Security and Privacy (CODASPY 2016, 2017)
ACM Symposium on Access Control Models and Technologies (SACMAT 2017, 2019, 2020)
ACM International Conference on Information and Knowledge Management (CIKM 2017)
International World Wide Web Conference (WWW 2019, 2020)

Volunteer & Web Master

SAC-PA Workshop 2017, 2018.
IEEE CIC 2016, 2017, 2018, 2019; IEEE TPS 2019; IEEE CogMI 2019; IEEE IRI 2016; IEEE Cloud 2016.

Intern & Teaching

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)
The Principle of Database System. School of Computer Science and Engineering, Beihang University. (2012 Spring)

Teaching Fellow

INFSCI 2150/TELCOM 2810 *Information Security and Privacy (Online).* School of Computing and Information, University of Pittsburgh. (2016 Summer, 2016 Fall, 2017 Summer, 2017 Fall, 2018 Summer)

Intern

2019.5-2019.8 Research Intern. *IBM Research - Almaden. San Jose, California, USA.*
2014.3-2014.12 Research and Development Engineer. *Department of Image Search, Baidu Inc. Beijing, China.*
2011.7-2011.8 Software Development Engineer. *National Software Talent International Training Base. Xi'an, Shannxi, China.*

Grants, Honors & Awards

2016 Student Travel Award, IEEE Cloud 2016.
2012-2013 The Scholarship of Graduate, Beihang University. (2 times)
2011 Honored enrollment granted mandatory admission test waived.
2008-2011 The Scholarship of Undergraduate, Northwestern Polytechnical University.(3 times)
2008-2011 Excellent Student Leaders Award, Merit Student Award, Northwestern Polytechnical University.

Last updated: October 25, 2020 • Typeset in LaTeX
xurunhua.com