SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Curriculum Vitae

Dr Xu Jia
Lecturer
School of Science and Technology

Tel : +65 6248 0467

Education Qualifications

2012	PhD in Computer Science, National University of Singapore
2006	Bachelor of Computer Science, National University of Singapore

Academic and Professional Experience

2023 – Present	Lecturer, School of Science and Technology, Singapore University of Social Sciences
2021 – 2023	Senior Research Fellow, The Asian Institute of Digital Finance, National University of Singapore
2017 – 2021	R&D Manager, NUS-SingTel Cyber Security Research & Development Laboratory, SingTel, Trustwave
2015 – 2017	Research Scientist II, Department of Infocomm Security, Institute for Infocomm Research, Singapore
2012 – 2015	Research Scientist, Department of Infocomm Security, Institute for Infocomm Research, Singapore
2010 – 2011	Research Assistant, Department of Computer Science, National University of Singapore

Teaching Experience

2017 – 2021	Supervisor from Industry, National University of Singapore, 2 Final Year Projects
2012 – 2017	Supervisor from Industry, Singapore Polytechnic, 4 Final Year Projects
2014	Supervisor, City University of Hong Kong, PhD student internship. Internship led to 2 research papers
2008 – 2009	Part-time Teaching Assistant, Department of Information System, National University of Singapore
2005 – 2006	Part-time Teaching Assistant, Department of Computer Science, National University of Singapore

SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Certifications

2019 – Present	Certified Information Systems Security Professional
2019 – Present	GIAC Certified Incident Handler

Research Interests

- Applied Cryptography
- Secure Cloud Computing, especially in cloud storage
- Post-Quantum Cryptography
- Privacy Preserving Computation
- Cyber-Physical Security
- Mobile Security

Research Areas

- Private Set Intersection and Privacy Preserving Biometric Authentication and Identification
- Privacy Leakage in Searchable Encryption Scheme
- Confidential Computing by Combining Crypto and Trusted hardware
- Hybrid Post-Quantum Key Exchange Protocol
- Proof of Ownership and Client-side Deduplication in Cloud Storage
- Proof of Storage scheme (Proofs of Retrievability and Provable Data Possession)
- Homomorphic Digital Signature and Tree Structure
- Design and Implement Security Apps for Smartphone
- Visually Isolated Network System

Research Grants

2018 – 2021	Lead PI, about 650K SGD, NRF (Post-Quantum Security as a Service)
2017 – 2022	co-PI, about 3.5M SGD, NRF (Quantum Key Distribution)
2017 – 2021	co-PI, about 750K SGD, NRF (Secure Cloud Service)

Patents

I have applied 3 provisional patents in (1) private set intersection, (2) remote software attestation, and (3) post-quantum key exchange protocol.

Selected Publications

Muhammad Naveed Aman, Haroon Basheer, Jun Wen Wong, Jia Xu, Hoon Wei Lim, and Biplab Sikdar. Machine-learning based attestation for the internet of things using memory traces. IEEE Internet of Things Journal, 9(20):20431-20443, 2022.

Muhammad Naveen Aman, Mohamed Haroon Basheer, Siddhant Dash, Ashutosh Sancheti, Jun Wen

Wong, Jia Xu, Hoon Wei Lim, and Biplab Sikdar. PRoM: Passive Remote Attestation Against Roving Malware in Multicore IoT Devices. IEEE Systems Journal, 2021.

Yiwen Gao, Jia Xu, and Hongbing Wang. cuNH: Efficient GPU Implementations of Post-Quantum KEM NewHope. Transactions on Parallel and Distributed Systems, 2021.

Muhammad Naveed Aman, Mohamed Haroon Basheer, Siddhant Dash, Jun Wen Wong, Jia Xu, Hoon Wei Lim, and Biplab Sikdar. HAtt: Hybrid Remote Attestation for the Internet of Things with High Availability. IEEE Internet of Things Journal, 7, 2020.

Jia-Chng Loh, Geong-Sen Poh, Jason H. M. Ying, Jia Xu, Hoon Wei Lim, Jonathan Pan, and Weiyang Wong. Pbio: Enabling cross-organizational biometric authentication service through secure sharing of biometric templates. Cryptology ePrint Archive, Report 2020/1381, 2020. https://eprint.iacr.org/2020/1381

Jia Xu and Jianying Zhou. Strong leakage-resilient encryption: enhancing data confidentiality by hiding partial ciphertext. International Journal of Information Security, 2020.

Jason H. M. Ying, Shuwei Cao, Geong Sen Poh, Jia Xu, and Hoon Wei Lim. Psi-stats: Private set intersection protocols supporting secure statistical functions. Cryptology ePrint Archive, Report 2020/623, 2020. https://eprint.iacr.org/2020/623

Jianting Ning, Xu, Jia, Kaitai Liang, Fan Zhang, and Ee-Chien Chang. Passive Attacks Against Searchable Encryption. IEEE Transactions on Information Forensics and Security, 14:789–802, March 2019.

Hoon Wei Lim, Geong Sen Poh, Jia Xu, and Varsha Chittawar. Privatelink : Privacypreserving integration and sharing of datasets. In IEEE Transactions on Information Forensics and Security, pages 564–577, 2019.

Jia Xu and Jianying Zhou. Strong leakage resilient encryption by hiding partial ciphertext. In Applied Cryptography and Network Security Workshops, pages 172–191, 2019.

Jia Xu and Jianying Zhou. Virtually Isolated Network: A Hybrid Network to Achieve High Level Security. In Data and Applications Security and Privacy XXXII, DBSec, pages 324–343, 2018.

A. Yang, J. Xu, J. Weng, J. Zhou, and D. S. Wong. Lightweight and Privacy-Preserving Delegatable Proofs of Storage with Data Dynamics in Cloud Storage. IEEE Transactions on Cloud Computing, 2018.

Dong Li, Huaqun Guo, and Jia Xu. Enhancing TPM Security by Integrating SRAM PUFs Technology. In ACM International Workshop on Cyber-Physical System Security, CPSS '16, pages 82–93, 2016.

Jia Xu, Ee-Chien Chang, and Jianying Zhou. Directed Transitive Signature on Directed Tree. In Singapore Cyber-Security Conference (short paper), SG-CRC, pages 91–98, 2016. Full version in http://eprint.iacr.org/2009/209.

Jia Xu, Anjia Yang, Jianying Zhou, and Duncan S. Wong. Lightweight Delegatable Proofs of Storage. In European Symposium on Research in Computer Security, ESORICS, pages 324–343, 2016.

http://eprint.iacr.org/2014/395.

Jia Xu, Jianying Zhou, and Liming Lu. Cyber and Physical Access Control in Legacy System Using Passwords. In Singapore Cyber-Security Conference, SG-CRC, pages 27–42, 2016. http://eprint.iacr.org/2015/1161.

Jia Xu and Jianying Zhou. Leakage Resilient Proofs of Ownership in Cloud Storage, Revisited. In Applied Cryptography and Network Security, ACNS, pages 97–115, 2014.

Cheng-Kang Chu, Wen-Tao Zhu, Jin Han, Joseph K. Liu, Jia Xu, and Jianying Zhou. Security Concerns in Popular Cloud Storage Services. IEEE pervasive computing, 12(4):50–57, 2013. **Citation Count: 105**.

Jia Xu, Ee-Chien Chang, and Jianying Zhou. Weak Leakage-resilient Client-side Deduplication of Encrypted Data in Cloud Storage. In ACM SIGSAC Symposium on Information, Computer and Communications Security, ASIA CCS '13, pages 195–206, 2013. **Citation Count: 263**.

Jia Xu and Ee-Chien Chang. Towards Efficient Proofs of Retrievability. In ACM Symposium on Information, Computer and Communications Security, ASIACCS (Full paper), 2012. **Citation Count: 111**.

Jie Yu, Zhoujun Li, Peng Xiao, Chengfang Fang, Jia Xu, and Ee-Chien Chang. ID Repetition in Structured P2P Networks. The Computer Journal, 54(6):962–975, 2011.

Ee-Chien Chang, Chengfang Fang, and Jia Xu. A chameleon encryption scheme resistant to known-plaintext attack. In ACM workshop on Digital rights management, DRM, pages 25–34, 2010.

Ee-Chien Chang, Chee Liang Lim, and Jia Xu. Short Redactable Signatures Using Random Trees. In The Cryptographers' Track at the RSA Conference on Topics in Cryptology, CTRSA, pages 133–147, 2009. **Citation Count: 81**.

Jie Yu, Chengfang Fang, Jia Xu, Ee-Chien Chang, and Zhoujun Li. ID Repetition in Kad. In Peer-to-Peer Computing, P2P, pages 111–120, 2009. **Citation Count: 39**.

Ee-Chien Chang and Jia Xu. Remote Integrity Check with Dishonest Storage Server. In European Symposium on Research in Computer Security, ESORICS, pages 223–237, 2008. **Citation Count: 137**.

Jia Xu and Zhiyong Huang. HOPI: A Novel High Order Parametric Interpolation in 2D (FYP Result). In Eurographics (short paper), pages 99–102, 2006.

Academic Activities

2006 – Present	PC Member, Inscrypt '14, SCC '15, SCC '16, CPSS '16, CPSS '17, SCC '17, ICICS '19, '20, '21, CloudCom '19, '20.
2006 – Present	Internal or external reviewer. TKDE, Information Hiding '09 '11, Pairing '10, ISC '11, SecureComm '11, ESORICS, ACNS, AsiaCCS, FC, CNS, ICICS, etc.
2006 – Present	Academic Conference Attended. ASIACCS '07, ESORICS '08, ASIACRYPT '10, ACNS '12, ASIACCS '13, ACNS '14, AsiaCCS '15, SG-CRC '16, ESORICS '16.

2006	First Prize in Mathematical Modeling Summer Camp. Joint-Organized by National University of Singapore and Peking University in China, Location: Singapore and Beijing.

Scholarships

2006 – 2010	PhD Research Scholarship, National University of Singapore, Singapore
2001 – 2006	SM3 PRC Scholarship, Ministry of Education, Singapore

Updated on 24 Nov 2023