

CURRICULUM VITAE

Personal Information			
Name	Shiwei Xu	Gender	Male
Position Title	Associate Professor		
Working Department	College of Informatics		
Email	xushiwei@mail.hzau.edu.cn		
Address	No. 1, Shizishan Street, Hongshan District, Wuhan, Hubei Province		
Tel	0086-15002787572	Fax	
Research Interest			
Blockchain Security, Data Security and Privacy, Applied Cryptography			
Professional Memberships			
CCF (China Computer Federation), IEEE member			
Other Roles			
Education & Working Experience			
College of Informatics, Huazhong Agriculture University	Aug. 2017 to now		
Wuhan Digital and Engineering Research Institute	Sep. 2012 to Jul. 2017		
PhD in Information Security, Wuhan University	Sep. 2008 – Jun. 2012		
Visiting PhD Student in Information Security, University of Birmingham, UK	Sep. 2010 – Mar. 2012		
MS in Information Security, Wuhan University	Sep. 2006 – Jun. 2008		
BS in Computer Science and Technology, Wuhan University	Sep. 2002 – Jun. 2006		
Publications			
<ul style="list-style-type: none">• Shiwei Xu, Ao Sun, Zhengwei Ren, Yizhi Zhao, Qiefen Ni, Yan Tong. “Enhanced post-quantum key escrow system for supervised data conflict of interest based on consortium blockchain”, Journal of Combinatorial Optimization, 2023, 45(6): 116• Yan Tong, Xiangyong Zeng, Shasha Zhang, Shiwei Xu, Zhengwei Ren. “The estimates of trigonometric sums and new bounds on a mean value, a sequence and a cryptographic function”, Designs, Codes and Cryptography, 2023, 91(3): 9210949• Zhengwei Ren, Xiaojuan Li, Lina Wang, Shiwei Xu, Yan Tong, Jinshan Tang. “Minimal key set of			

binary key-derivation tree in cloud storage”, *Soft Computing*, 2023, 27(2): 1177-1188

- **Shiwei Xu**, Xiaowen Cai, Yizhi Zhao, et al. “zkrcChain: Towards Multi-party Privacy-preserving Data Auditing for Consortium Blockchains Based on Zero-knowledge Range Proofs,” *Future Generation Computer System*, 2022, 128: 490-504
- Zhengwei Ren, Xueting Li, Li Deng, Yan Tong, **Shiwei Xu**, Jinshan Tang. “RAS2P: Remote Attestation via Self-Measurement for SGX-based Platforms”, in Proc. SMC, Czech Republic, 2022
- **Shiwei Xu**, Ao Sun, Xiaowen Cai, et al. “Post-Quantum User Authentication and Key Exchange in Consortium Blockchain Systems,” in Proc. ICPADS, Beijing, China, 2021
- Xiaowen Cai, Wenjing Cheng, Minghui Zhang, Chen Qian, Zhengwei Ren, **Shiwei Xu***, Jianying Zhou. “Post-quantum Key Escrow for Supervised Secret Data Sharing on Consortium Blockchain,” in Proc. CSS, Copenhagen, Denmark, 2021
- Zhengwei Ren, Xiaoshuang Chen, Jinshan Tang, Lina Wang, Yan Tong, **Shiwei Xu**. “Limited Times of Data Access Based on SGX in Cloud Storage”, in Proc. SMC, Melbourne, Australia, 2021
- **Shiwei Xu**, Yizhi Zhao, Zhengwei Ren, et al. “A Symbolic Model for Systematically Analyzing TEE-based Protocols,” in Proc. ICICS, Copenhagen, Denmark, 2020 (**Best paper awarded**)
- **Shiwei Xu**, Xiaowen Cai, Yizhi Zhao, et al. “zkrcChain: Privacy-preserving Data Auditing for Consortium Blockchains Based on Zero-knowledge Range Proofs,” in Proc. TrustCom, Guangzhou, China, 2020