

# Yongjun Zhao 赵永骏

Research Scientist - TikTok  
Homepage: <https://yongjunzhao.github.io/>

Email: [foreverjun.zhao@gmail.com](mailto:foreverjun.zhao@gmail.com)  
ORCID: 0000-0001-7380-3806

## Work Experience

|                                               |                                                                                                                      |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Research Scientist<br>(12/2022 – present)     | TikTok<br>Privacy Innovation Lab                                                                                     |
| Senior Research Fellow<br>(07/2022 – 11/2022) | Strategic Centre for Research in Privacy-Preserving Technologies and Systems (SCRiPTS)                               |
| Research Fellow<br>(10/2019 – 06/2022)        | Nanyang Technological University, Singapore                                                                          |
| Research Assistant<br>(09/2018 – 08/2019)     | Department of Information Engineering<br>The Chinese University of Hong Kong, Hong Kong SAR, China                   |
| Part-time Instructor<br>(01/2017 – 05/2017)   | IEMS5710 Cryptography, Information Security and Privacy<br>The Chinese University of Hong Kong, Hong Kong SAR, China |

## Education

|                   |                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 09/2013 – 06/2018 | The Chinese University of Hong Kong, Hong Kong SAR, China<br>Ph.D. in Information Engineering<br><b>Dissertation:</b> Privacy Enhancing Technologies: New Primitives and New Systems<br><b>Advisor:</b> Sherman S. M. Chow |
| 09/2011 – 06/2013 | The Chinese University of Hong Kong, Hong Kong SAR, China<br>B.Eng. in Information Engineering, First Class Honor                                                                                                          |
| 09/2009 – 06/2011 | Sun Yat-sen University, Guangzhou, China                                                                                                                                                                                   |

## Research Interests

1. Privacy-enhancing technologies (Set Operations, Machine Learning, Cryptocurrency/E-cash, etc.)
2. Cryptographic solutions for cloud storage system (Searchable Encryption, Proofs of Retrievability (PoR), Proofs of Ownership (PoW), Message-Locked Encryption (MLE), etc.)
3. Digital signatures and anonymous authentication

## Publications by Topics

### *Private Set Operations*

1. Wenjie Lu, Yongchuan Niu, **Yongjun Zhao**, Wei Dai, Donghang Lu, and Qiang Yan. Secure join operations in multi-identifier databases: Performance and practicality. *VLDB*, 2026 (to appear).
2. Chenyu Huang, Fan Zhang, Huangxun Chen, **Yongjun Zhao**, Huaming Rao, Peng Chen, and Danqing Huang. Privacy-preserving screening for record linkage. In *41st IEEE International Conference on Data Engineering, ICDE 2025, Hong Kong, May 19-23, 2025*, pages 3751–3764. IEEE, 2025.
3. Jingwei Hu, **Yongjun Zhao**, Benjamin Hong Meng Tan, Khin Mi Mi Aung, and Huaxiong Wang. Enabling threshold functionality for private set intersection protocols in cloud computing. *IEEE Trans. Inf. Forensics Secur.*, 19:6184–6196, 2024.
4. **Yongjun Zhao** and Sherman S. M. Chow. Can you find the one for me? privacy-preserving matchmaking via

threshold PSI. In *Proceedings of the 2018 Workshop on Privacy in the Electronic Society, WPES@CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 54–65, 2018.

5. **Yongjun Zhao** and Sherman S. M. Chow. Are you the one to share? secret transfer with access structure. *Proc. Priv. Enhancing Technol.*, 2017(1):149–169, 2017.

### ***Advanced Signatures and Credentials***

1. Yingfei Yan, Sherman S. M. Chow, Lucien K. L. Ng, Harry W. H. Wong, **Yongjun Zhao**, and Baocang Wang. Batch anonymous MAC tokens from lattices. In Ruben Niederhagen and Markku-Juhani O. Saarinen, editors, *Post-Quantum Cryptography - 16th International Workshop, PQCrypto 2025, Taipei, Taiwan, April 8-10, 2025, Proceedings, Part I*, volume 15577 of *Lecture Notes in Computer Science*, pages 349–384. Springer, 2025.
2. Yingfei Yan, **Yongjun Zhao**, Wen Gao, and Baocang Wang. Lattice-based threshold, accountable, and private signature. In *Topics in Cryptology - CT-RSA 2024 - Cryptographers' Track at the RSA Conference 2024, San Francisco, CA, USA, May 6-9, 2024, Proceedings*, volume 14643 of *Lecture Notes in Computer Science*, pages 249–274. Springer, 2024.
3. Sherman S. M. Chow, Alexander Russell, Qiang Tang, Moti Yung, **Yongjun Zhao**, and Hong-Sheng Zhou. Let a non-barking watchdog bite: Cliptographic signatures with an offline watchdog. In *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part I*, volume 11442 of *Lecture Notes in Computer Science*, pages 221–251, 2019.

### ***Cryptographic Privacy-preserving Machine Learning***

1. Yu Zheng, Wei Song, Minxin Du, Sherman S.M. Chow, Qian Lou, **Yongjun Zhao**, and Xiuhua Wang. Cryptography-inspired federated learning variants for gan and meta learning. In *Advanced Data Mining and Applications - 19th International Conference, ADMA 2023, Proceedings*, Lecture Notes in Computer Science, 2023.
2. Lucien K. L. Ng, Sherman S. M. Chow, Anna P. Y. Woo, Donald P. H. Wong, and **Yongjun Zhao**. Goten: Gpu-outsourcing trusted execution of neural network training. In *Thirty-Fifth AAAI Conference on Artificial Intelligence, AAAI 2021, Thirty-Third Conference on Innovative Applications of Artificial Intelligence, IAAI 2021, The Eleventh Symposium on Educational Advances in Artificial Intelligence, EAAI 2021, Virtual Event, February 2-9, 2021*, pages 14876–14883. AAAI Press, 2021.
3. Jack P. K. Ma, Raymond K. H. Tai, **Yongjun Zhao**, and Sherman S. M. Chow. Let's stride blindfolded in a forest: Sublinear multi-client decision trees evaluation. In *28th Annual Network and Distributed System Security Symposium, NDSS*. The Internet Society, 2021.
4. Raymond K. H. Tai, Jack P. K. Ma, **Yongjun Zhao**, and Sherman S. M. Chow. Privacy-preserving decision trees evaluation via linear functions. In *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*, volume 10493 of *Lecture Notes in Computer Science*, pages 494–512, 2017.
5. **Yongjun Zhao** and Sherman S. M. Chow. Privacy preserving collaborative filtering from asymmetric randomized encoding. In *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers*, volume 8975 of *Lecture Notes in Computer Science*, pages 459–477, 2015.

### ***Cryptographic Solution for Cloud Storage System***

1. Ivan Tjuawinata, **Yongjun Zhao**, Bowen Shen, Kwok-Yan Lam, and Chi-Hung Chi. Search and permission request over encrypted database. In *The 10th International Conference on ICT for Smart Society 2023 (ICISS 2023), September 6-7, 2023, Bandung, Indonesia, 2023*.
2. **Yongjun Zhao** and Sherman S. M. Chow. Updatable block-level message-locked encryption. *IEEE Trans. Dependable Secur. Comput.*, 18(4):1620–1631, 2021.
3. Sherman S. M. Chow and **Yongjun Zhao**. Secure data deduplication schemes. *Encyclopedia of Cryptography, Security and Privacy*, pages 1–4, 2019.
4. **Yongjun Zhao** and Sherman S. M. Chow. Updatable block-level message-locked encryption. In *Proceedings*

of the 2017 ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2-6, 2017, pages 449–460, 2017.

5. **Yongjun Zhao** and Sherman S. M. Chow. Towards proofs of ownership beyond bounded leakage. In *Provable Security - 10th International Conference, ProvSec 2016, Nanjing, China, November 10-11, 2016, Proceedings*, volume 10005 of *Lecture Notes in Computer Science*, pages 340–350, 2016.

## Blockchain

1. Chenyu Huang, **Yongjun Zhao**, Huangxun Chen, Xu Wang, Qian Zhang, Yanjiao Chen, Huaxiong Wang, and Kwok-Yan Lam. zkrep: A privacy-preserving scheme for reputation-based blockchain system. *IEEE Internet of Things Journal*, 9(6):4330–4342, 2022.
2. Sherman S. M. Chow, Ziliang Lai, Chris Liu, Eric Lo, and **Yongjun Zhao**. Sharding blockchain. In *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), iThings/GreenCom/CPSCom/SmartData 2018, Halifax, NS, Canada, July 30 - August 3, 2018*, page 1665, 2018.
3. Weizhi Meng, Jianfeng Wang, Xianmin Wang, Joseph K. Liu, Zuoxia Yu, Jin Li, **Yongjun Zhao**, and Sherman S. M. Chow. Position paper on blockchain technology: Smart contract and applications. In *Network and System Security - 12th International Conference, NSS 2018, Hong Kong, China, August 27-29, 2018, Proceedings*, volume 11058 of *Lecture Notes in Computer Science*, pages 474–483, 2018.

## Privacy-preserving Payment Systems

1. Sherman S. M. Chow, Ming Li, **Yongjun Zhao**, and Wenqiang Jin. Sipster: Settling IOU privately and quickly with smart meters. In *ACSAC '21: Annual Computer Security Applications Conference, Virtual Event, USA, December 6 - 10, 2021*, pages 219–234. ACM, 2021.
2. Sherman S. M. Chow, Russell W. F. Lai, Xiuhua Wang, and **Yongjun Zhao**. Privacy preserving credit systems. In *Network and System Security - 10th International Conference, NSS 2016, Taipei, Taiwan, September 28-30, 2016, Proceedings*, volume 9955 of *Lecture Notes in Computer Science*, pages 184–199, 2016.

## Manuscripts

1. Jian Du, Haohao Qian, Bo Jiang, Donghang Lu, Shikun Zhang, Wenjie Lu, Donghang Lu, Bo Jiang, **Yongjun Zhao**, and Qiang Yan. Privacy-preserving ad measurement with multidimensional intersection. *Manuscript*, 2025.
2. Yingfei Yan, Sherman S. M. Chow, Stella Wahnig, **Yongjun Zhao**, and Baocang Wang. Versatile anonymous tokens with seamless metadata channels. *Manuscript*, 2024.
3. **Yongjun Zhao**, Huaxiong Wang, and Kwok-Yan Lam. Volume-hiding dynamic searchable symmetric encryption with forward and backward privacy. *IACR Cryptol. ePrint Arch.*, page 786, 2021.

## Patents

1. Jian Du, Haohao Qian, **Yongjun Zhao**, Bo Jiang, and Qiang YAN. Protecting membership and data in a secure multi-party computation and/or communication, January 30 2024. US Patent 11,886,617.
2. Jian Du, **Yongjun Zhao**, Haohao Qian, Bo Jiang, and Qiang YAN. Protecting membership in a secure multi-party computation and/or communication, May 21 2024. US Patent 11,989,325.
3. **Yongjun Zhao**, Jian Du, Haohao Qian, Bo Jiang, and YAN Qiang. Secure computation and communication, November 7 2023. US Patent 11,811,920.
4. Jian Du, **Yongjun Zhao**, Haohao Qian, Bo Jiang, and Qiang YAN. Protecting membership in a secure multi-party computation and/or communication, November 28 2023. US Patent 11,829,512.
5. Bo Jiang, Jian Du, Haohao Qian, **Yongjun Zhao**, and Qiang YAN. Fast convolution algorithm for composition determination, January 9 2024. US Patent 11,868,497.
6. Jian Du, Haohao Qian, **Yongjun Zhao**, Bo Jiang, Chuyuan Chen, and Qiang YAN. Secure multi-party computation and communication, December 5 2023. US Patent 11,836,263.

7. Jian Du, Haohao Qian, **Yongjun Zhao**, Bo Jiang, Chuyuan Chen, and Qiang YAN. Secure multi-party computation and communication, May 14 2024. US Patent 11,983,285.

## Professional Activities

### Session Chair:

2023: ACM CCS  
2021: Asisacrypt

### Program Committee:

2026: AAAI  
2025: AAAI, IEEE Global Blockchain Conference  
2024: AAAI, PPAI, ICDCS  
2023: AAAI (Main Track & AI for Social Impact Track), PoPETs  
2022: AAAI (AI for Social Impact Track), EAI AC3, ICICS, PoPETs, SACMAT, SeCrypt, UbiSec, USENIX Security Artifact Evaluation  
2021: APKC, DPML, EAI AC3, ICICS, ISPEC, IEEE S&P (Shadow PC), PoPETs, SeCrypt, TrustCom, UbiSec, USENIX Security Artifact Evaluation  
2020: Globecom CISS, ISPEC, NSS, SECrypt, TrustCom  
2019: 3ICT, C2SI, Globecom CISS, ICPADS, SECrypt  
2018: AsiaCCS-SCC, BlockSEA, NSS, SECrypt, SecureComm  
2017: CANS, InsCrypt, SECrypt, Cyber Security (CS)

### External Reviewer:

2026: IEEE TETC, IEEE TPDS  
2025: IEEE TDSC, IEEE TGCN, IEEE TIFS  
2024: CRYPTO, IEEE TCC, IEEE TDSC  
2023: IEEE TIFS, IEEE TDSC  
2022: ACNS, AsiaCCS, CCS, CT-RSA, ESORICS, IWSEC, IEEE Systems Journal, IET Information Security, The Computer Journal  
2021: AsiaCCS, ESORICS, EuroS&P, ICDCS, PKC, PoPETs, USENIX Security, ACM TOPS, IEEE TDSC, IET Information Security  
2020: ACNS, AsiaCCS, AsiaCrypt, ESORICS, IEEE TC, IEEE TCC, Sensors, The Computer Journal  
2019: ACNS, AsiaCCS, AsiaCrypt, CNS, CRYPTO, ESORICS, ISC, ISPEC, PoPETS, SecureComm, IEEE TCC, FGCS, JISA  
2018: AsiaCCS, AfricaCrypt, CNS, ESORICS, ICICS, ISC, PoPETS, PST, Computer Networks (SI), IEEE TIFS, IEEE TCC, FGCS  
2017: ACNS, AsiaCrypt, AfricaCrypt, AsiaCCS, AsiaCCS-APKC, AsiaCCS-SCC, C2SI, ESORICS, Globecom, ISC, PST, SACMAT, WPES, CoSe, JISA  
2016: ACNS, AfricaCrypt, AsiaCCS, AsiaCrypt, APKC, CANS, CNS, ESORICS, Globecom, ICC, ICPADS, Inscrypt, ISC, ISPEC, POST, SACMAT, SecureComm, WPES, Computer & Security, IJIS  
2015: AsiaCCS, AsiaCrypt, CNS, CANS, Financial Crypt, ICDCS, ICICS, Infocom, InsCrypt, ISC, PKC, SECrypt, SmartGridComm, PerCom  
2014: ACM-CCS, AsiaCCS, AsiaPKC, AsiaCrypt, CNS, ESORICS, HPCC, ICICS, ISC, ISPEC, SmartGridComm  
2013: InsCrypt

## Seminars and Talks

- [July 2025] [Lightning Talks: Making PETs Work for You](#)  
PETs Summit - Redefining what's possible with Privacy Enhancing Technologies, Singapore
- [Aug 2024] [Challenges in Privacy and Security of Generative AI Models](#)  
The Trustworthy Data Science and AI (TDSAI) Lab, Tokyo Institute of Technology, Japan
- [Jul 2024] [Synergizing DP and MPC for Privacy-Preserving Ad Measurement](#)  
Privacy-Enhancing Technology Summit Asia-Pacific 2024, Singapore

- [Jul 2024] [PrivacyGo: TikTok's Initiative in Synergistic PETs](#)  
STACK Meetup, GovTech, Singapore
- [Sep 2023] [Protecting User Privacy in Private Set Intersection: A Journey Toward Mitigating User Tracking](#)  
School of Computing, National University of Singapore
- [Sep 2023] [Protecting User Privacy in Private Set Intersection: A Journey Toward Mitigating User Tracking](#)  
School of Computing & Information Systems, Singapore Management University
- [Aug 2022] [Private Set Intersection: Introduction and Applications](#)  
Joint Workshop by ISACA SG, IAPP SG Knowledge Net and NTU
- [May 2022] [Towards Efficient and Practical Privacy-Preserving Machine](#)  
Department of Computing, The Hong Seng University of Hong Kong

## Honors and Awards

Runner-up Prize (Collaboration with AngelPowerFL, Tencent), iDASH Privacy & Security Workshop 2022 - Secure Genome Analysis Competition, Track 4: Secure Record Linkage  
[Top Reviewer Award](#), The 22nd Privacy Enhancing Technologies Symposium  
[Outstanding Tutors Awards 2016](#), Faculty of Engineering, CUHK  
 Teaching Assistant Award for 1st Term 2016-17, Dept. of Information Engineering, CUHK  
 Teaching Assistant Award for 2nd Term 2015-16, Dept. of Information Engineering, CUHK  
 Dean's List 2012/2013, Faculty of Engineering, CUHK  
 Dean's List 2011/2012, Faculty of Engineering, CUHK  
 Chung Chi College Departmental Prize 2011/2012, CUHK (HK\$ 10,000)  
 Chung Chi College Scholarship 2011/2012, CUHK (HK\$ 2,000)  
 National Scholarship for 2010/2011, Sun Yat-sen University (RMB¥ 8,000)  
 The First Prize scholarship of SYSU Scholarship Fund for 2010/2011, Sun Yat-sen University (RMB¥ 2,000)  
 The Third Prize scholarship of SYSU Scholarship Fund for 2009/2010, Sun Yat-sen University (RMB¥ 1,000)

## Teaching Experience

### Nanyang Technological University

RE4001: Renaissance Capstone Project (co-supervise with Prof Lam Kwok Yan)  
 Project title: [Privacy-preserving matchmaking in social networks](#)  
 Students: Ho, Alexander Joong Khuan, Lim, Collin Tian Jun, Wong, Vincent Yong Sheng  
 PS101: Introduction to Privacy-preserving Secure Data Computation & Analytics (Instructor)

### The Chinese University of Hong Kong

IERG2051 Signals and Systems, CUHK (Teaching Assistant)  
 IERG3310 Computer Networks, CUHK (Teaching Assistant)  
 IERG4130 Introduction to Cyber Security, CUHK (Teaching Assistant, Outstanding TA Award)  
 IERG4160 Image and Video Processing, CUHK (Teaching Assistant)  
 IEMS5710 Cryptography, Information Security and Privacy, CUHK (Part-time Instructor)

## Skills

- Programming Languages: Latex, C/C++, Python, Java, C#, Web Programming, Matlab
- Languages: Cantonese (native), English (fluent), Mandarin (fluent)