📱 *+61-88538287*
✉ *zuocong10@gmail.com*
🌐 *zuocong10.github.io*
Google Scholar: https://scholar.google.com/citations?user=XvE1w8kAAAAJ&hl=en

Cong Zuo

Education

2017.05∼ 2020.11 **Ph.D. in Security Science (Cybersecurity)**, *Faculty of Information Technology, Monash University*, Australia.

- Supervisor: Asso. Prof. Joseph.K. Liu
- Co-supervisor: Dr. Shifeng Sun, Prof. Josef Pieprzyk

2013.09∼ 2016.06 **Master in Computer Science**, *School of Computer and Information Engineering, Zhejiang Gongshang University*, Hangzhou, Zhejiang, China.

- GPA: 86/100
- Supervisor: Prof. Jun Shao

2009.09∼ 2013.06 **Bachelor in Computer Science and Technology**, *School of Computer Science, Nanjing Institute of Technology*, Nanjing, Jiangsu, China.

- GPA: 83/100
- Supervisor: Sheng Liu

Research Interest

Searchable Symmetric Encryption, Database Security, Data Privacy, Applied Cryptography.

Work Experience

2021.01∼ Present **Postdoctor**, Nanyang Technological University.

2019.02∼ 2020.06 **Teaching Associate**, *Faculty of Information Technology*, Monash University.

- Improve lab materials and conduct tutorials as well as consultations for FIT 3173 (Semester 1 of 2019, Semester 1 of 2020)

Service

Invited Reviewer.

- The Computer Journal
- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Services Computing (TSC)
- The 25th Australasian Conference on Information Security and Privacy (ACISP 2020)
- The 21st International Conference on Information and Communications Security (ICICS 2019)

Session Chair.

- The 13th International Conference on Provable and Practical Security (PROVSEC 2019)
- The 13th International Conference on Network and System Security (NSS 2019)
- The 18th Annual International Conference on Privacy, Security and Trust (PST2021)

Technical Program Committee.

- The 2022 IEEE International Conference on Communications (ICC): SAC E-Health Track
- The 18th Annual International Conference on Privacy, Security and Trust (PST2021)
- The 15th International Conference on Provable and Practical Security (PROVSEC 2021)
- The 17th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (EAI QSHINE 2021)
- The 13th EAI International Conference on Ad Hoc Networks (EAI ADHOCNETS 2021)

Assistant Guest Editor.

- Special issue in MDPI Cryptography: Emerging Cryptographic Protocols for Blockchain and Its Applications

Publications

(Ranking according to CORE, CCF, and SCI. The Computing Research and Education Association of Australasia, China Computer Federation, Science Citation Index)

[1] **Cong Zuo**, Shi-Feng Sun, Joseph K. Liu, Jun Shao, Josef Pieprzyk, and Lei Xu. Forward and backward private dsse for range queries. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, accepted for publication, (**CORE A, CCF A, IF=6.404**).

[2] Shi-Feng Sun, **Cong Zuo**, Joseph K. Liu, Amin Sakzad, Ron Steinfeld, Tsz Hon Yuen, Xingliang Yuan, and Dawu Gu. Non-interactive multi-client searchable encryption: Realization and implementation. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, accepted for publication, (**CORE A, CCF A, IF=6.404**).

[3] Shabnam Kasra Kermanshahi, Joseph K. Liu, Ron Steinfeld, Surya Nepal, Shangqi Lai, Randolph Loh, and **Cong Zuo**. Multi-client cloud-based symmetric searchable encryption. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, accepted for publication, (**CORE A, CCF A, IF=6.404**).

[4] Lei Xu, Shi-Feng Sun, Xingliang Yuan, Joseph K. Liu, **Cong Zuo**, and Chungen Xu. Enabling authorized encrypted search for multi-authority medical databases. *IEEE Transactions on Emerging Topics in Computing (TETC)*, accepted for publication, (**SCI Q2, IF=4.989**).

[5] Lei Xu, Chungen Xu, Joseph K. Liu, **Cong Zuo**, and Peng Zhang. Building a dynamic searchable encrypted medical database for multi-client. *Information Sciences*, 527:394–405, 2020, (**CORE A, CCF B, SCI Q1, IF=5.910**).

[6] Qingqing Gan, **Cong Zuo**, Jianfeng Wang, Shi-Feng Sun, and Xiaoming Wang. Dynamic searchable symmetric encryption with forward and backward privacy: A

survey. In *Network and System Security (NSS)*, pages 37–52, Cham, 2019, (**CORE B**).

[7] **Cong Zuo**, Shi-Feng Sun, Joseph K. Liu, Jun Shao, and Josef Pieprzyk. Dynamic searchable symmetric encryption with forward and stronger backward privacy. In *Computer Security - 24th European Symposium on Research in Computer Security (ESORICS)*, pages 283–303, 2019 (**CORE A, CCF B**).

[8] Randolph Loh, **Cong Zuo**, Joseph K. Liu, and Shi-Feng Sun. A multi-client dsse scheme supporting range queries. In *International Conference on Information Security and Cryptology (Inscrypt)*, pages 289–307, 2018, (**CORE B**).

[9] Zhimei Sui, Shangqi Lai, **Cong Zuo**, Xingliang Yuan, Joseph K. Liu, and Haifeng Qian. An encrypted database with enforced access control and blockchain validation. In *International Conference on Information Security and Cryptology (Inscrypt)*, pages 260–273, 2018, (**CORE B**).

[10] Shangqi Lai, Sikhar Patranabis, Amin Sakzad, Joseph K. Liu, Debdeep Mukhopadhyay, Ron Steinfeld, Shifeng Sun, Dongxi Liu, and **Cong Zuo**. Result pattern hiding searchable encryption for conjunctive queries. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 745–762, 2018, (**CORE A*, CCF A**).

[11] **Cong Zuo**, Shifeng Sun, Joseph K. Liu, Jun Shao, and Josef Pieprzyk. Dynamic searchable symmetric encryption schemes supporting range queries with forward (and backward) security. In *Computer Security - 23rd European Symposium on Research in Computer Security (ESORICS)*, pages 228–246, 2018, (**CORE A, CCF B**).

[12] **Cong Zuo**, Jun Shao, Joseph K. Liu, Guiyi Wei, and Yun Ling. Fine-grained two-factor protection mechanism for data sharing in cloud storage. *IEEE Trans. Information Forensics and Security (TIFS)*, 13(1):186–196, 2018, (**CORE A, CCF A, IF=6.211**).

[13] **Cong Zuo**, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji. Cca-secure ABE with outsourced decryption for fog computing. *Future Generation Computer Systems (FGCS)*, 78:730–738, 2018, (**CORE A, CCF C, SCI Q2, ESI, IF=5.768**).

[14] Xinxin Ma, Jun Shao, **Cong Zuo**, and Ru Meng. Efficient certificate-based signature and its aggregation. In *Information Security Practice and Experience - 13th International Conference (ISPEC)*, pages 391–408, 2017, (**CORE B**).

[15] Lei Xu, Chungen Xu, Joseph K. Liu, **Cong Zuo**, and Peng Zhang. A multi-client dynamic searchable symmetric encryption system with physical deletion. In *Information and Communications Security - 19th International Conference (ICICS)*, pages 516–528, 2017, (**CORE B, CCF C**).

[16] **Cong Zuo**, Kaitai Liang, Zoe L. Jiang, Jun Shao, and Jun-bin Fang. Cost-effective privacy-preserving vehicular urban sensing system. *Personal and Ubiquitous Computing*, 21(5):893–901, 2017, (**CORE B, IF=2.0**).

[17] **Cong Zuo**, Jun Shao, Zhe Liu, Yun Ling, and Guiyi Wei. Hidden-token searchable public-key encryption. In *2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, August 1-4, 2017*, pages 248–254, 2017, (**CORE A, CCF C**).

[18] **Cong Zuo**, James Macindoe, Siyin Yang, Ron Steinfeld, and Joseph K. Liu. Trusted boolean search on cloud using searchable symmetric encryption. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 113–120, 2016, (**CORE A, CCF C**).

[19] **Cong Zuo**, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji. Chosen ciphertext secure attribute-based encryption with outsourced decryption. In *Information Security and Privacy - 21st Australasian Conference (ACISP)*, pages 495–508, 2016, (**CCF C**).

[20] Jun Shao, Xiaodong Lin, Rongxing Lu, and **Cong Zuo**. A threshold anonymous authentication protocol for vanets. *IEEE Transactions on Vehicular Technology*, 65(3):1711–1720, 2016, (**SCI Q2, IF=5.339**).

[21] Jun Shao, Rongxing Lu, Xiaodong Lin, and **Cong Zuo**. New threshold anonymous authentication for vanets. In *2015 IEEE/CIC International Conference on Communications in China*, pages 1–6, 2015.

Prizes & Awards

2017∼2020 **Data61 PhD & Supplementary Scholarship**, Data61, Commonwealth Scientific and Industrial Research Organization (CSIRO).

2017∼2020 **International Postgraduate Research Scholarship**, Monash University.

2016 **Guangming Wang ScholarshipZhejiang Gongshang University**, Zhejiang Gongshang University.

2013 **Excellent Undergraduate Student**, Nanjing Institute of Technology.

2012 **College-level Merit Student**, Nanjing Institute of Technology.

Co-Supervised Master Students

2018 **Randolph Loh**, he was a master student of Monash University. I co-supervised him, and we had a joint paper at International Conference on Information Security and Cryptology (Inscrypt), 2018 [8].

2018 **Zhimei Sui**, she was a master student of East China Normal University, and she visited Monash University in 2018. During her visit, I co-supervised her, and we also had a joint paper at International Conference on Information Security and Cryptology (Inscrypt), 2018 [9].

Referees

Associate Professor Joseph K. Liu, *Monash University, Australia*, joseph.liu@monash.edu.

Professor Jun Shao, *Zhejiang Gongshang University, China*, chn.junshao@gmail.com.

Professor Josef Pieprzyk, *Senior Principal Research Scientist in Data61, CSIRO, Australia*, Josef.Pieprzyk@data61.csiro.au.

Cong Zuo

Nanyang Technological University

Cryptography

GET MY OWN PROFILE

	All	Since 2017
Citations	702	683
h-index	10	10
i10-index	11	11

13 articles not available

7 articles available

Based on funding mandates

TITLE	CITED BY	YEAR
A threshold anonymous authentication protocol for VANETs J Shao, X Lin, R Lu, C Zuo IEEE Transactions on vehicular technology 65 (3), 1711-1720	220	2015
CCA-secure ABE with outsourced decryption for fog computing C Zuo, J Shao, G Wei, M Xie, M Ji Future Generation Computer Systems 78, 730-738	123	2018
Result pattern hiding searchable encryption for conjunctive queries S Lai, S Patranabis, A Sakzad, JK Liu, D Mukhopadhyay, R Steinfeld, ... Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications …	76	2018
Fine-grained two-factor protection mechanism for data sharing in cloud storage C Zuo, J Shao, JK Liu, G Wei, Y Ling IEEE Transactions on Information Forensics and Security 13 (1), 186-196	50	2017
Dynamic searchable symmetric encryption schemes supporting range queries with forward (and backward) security C Zuo, SF Sun, JK Liu, J Shao, J Pieprzyk European Symposium on Research in Computer Security, 228-246	43	2018
Privacy-preserving COVID-19 contact tracing app: a zero-knowledge proof approach JK Liu, MH Au, TH Yuen, C Zuo, J Wang, A Sakzad, X Luo, L Li, ... Cryptology ePrint Archive	39	2020
Dynamic searchable symmetric encryption with forward and stronger backward privacy C Zuo, SF Sun, JK Liu, J Shao, J Pieprzyk European Symposium on Research in Computer Security, 283-303	34	2019
Trusted boolean search on cloud using searchable symmetric encryption C Zuo, J Macindoe, S Yang, R Steinfeld, JK Liu 2016 IEEE Trustcom/BigDataSE/ISPA, 113-120	27	2016
Building a dynamic searchable encrypted medical database for multi-client L Xu, C Xu, JK Liu, C Zuo, P Zhang Information Sciences 527, 394-405	14	2020
New threshold anonymous authentication for VANETs J Shao, R Lu, X Lin, C Zuo 2015 IEEE/CIC International Conference on Communications in China (ICCC), 1-6	12	2015

TITLE	CITED BY	YEAR
Forward and backward private dsse for range queries C Zuo, S Sun, JK Liu, J Shao, J Pieprzyk, L Xu IEEE Transactions on Dependable and Secure Computing	10	2020
Enabling authorized encrypted search for multi-authority medical databases L Xu, S Sun, X Yuan, JK Liu, C Zuo, C Xu IEEE Transactions on Emerging Topics in Computing	7	2019
Cost-effective privacy-preserving vehicular urban sensing system C Zuo, K Liang, ZL Jiang, J Shao, J Fang Personal and Ubiquitous Computing 21 (5), 893-901	7	2017
Efficient certificate-based signature and its aggregation X Ma, J Shao, C Zuo, R Meng International Conference on Information Security Practice and Experience …	6	2017
Multi-client cloud-based symmetric searchable encryption SK Kermanshahi, JK Liu, R Steinfeld, S Nepal, S Lai, R Loh, C Zuo IEEE Transactions on Dependable and Secure Computing	5	2019
Chosen ciphertext secure attribute-based encryption with outsourced decryption C Zuo, J Shao, G Wei, M Xie, M Ji Australasian Conference on Information Security and Privacy, 495-508	5	2016
Dynamic searchable symmetric encryption schemes supporting range queries with forward/backward privacy C Zuo, SF Sun, JK Liu, J Shao, J Pieprzyk arXiv preprint arXiv:1905.08561	4	2019
A multi-client DSSE scheme supporting range queries R Loh, C Zuo, JK Liu, SF Sun International Conference on Information Security and Cryptology, 289-307	4	2018
Non-Interactive Multi-Client Searchable Encryption: Realization and Implementation SF Sun, C Zuo, JK Liu, A Sakzad, R Steinfeld, TH Yuen, X Yuan, D Gu IEEE Transactions on Dependable and Secure Computing	3	2020
An encrypted database with enforced access control and blockchain validation Z Sui, S Lai, C Zuo, X Yuan, JK Liu, H Qian International Conference on Information Security and Cryptology, 260-273	3	2018
hpress: A hardware-enhanced proxy re-encryption scheme using secure enclave F Zhang, Z Liang, C Zuo, J Shao, J Ning, J Sun, JK Liu, Y Bao IEEE Transactions on Computer-Aided Design of Integrated Circuits and …	2	2020
Forward and backward private dynamic searchable symmetric encryption for conjunctive queries C Zuo, SF Sun, JK Liu, J Shao, J Pieprzyk, G Wei Cryptology ePrint Archive	2	2020

TITLE	CITED BY	YEAR
A multi-client dynamic searchable symmetric encryption system with physical deletion L Xu, C Xu, JK Liu, C Zuo, P Zhang International Conference on Information and Communications Security, 516-528	2	2017
Hidden-Token Searchable Public-Key Encryption C Zuo, J Shao, Z Liu, Y Ling, G Wei 2017 IEEE Trustcom/BigDataSE/ICESS, 248-254	2	2017
Searchable Encryption with Access Control on Keywords in Multi-User Setting L Li, C Xu, X Yu, B Dou, C Zuo Journal of Cybersecurity 2 (1), 9	1	2020
Dynamic Searchable Symmetric Encryption with Forward and Backward Privacy: A Survey Q Gan, C Zuo, J Wang, SF Sun, X Wang International Conference on Network and System Security, 37-52	1	2019
Privacy-Preserving Contact Tracing Protocol for Mobile Devices: A Zero-Knowledge Proof Approach JK Liu, MH Au, TH Yuen, C Zuo, J Wang, A Sakzad, X Luo, L Li, ... International Conference on Information Security Practice and Experience …		2021
IoT Services: Realizing Private Real-Time Detection via Authenticated Conjunctive Searchable Encryption C Xu, M Lin, J Cheng, Y Zhao, C Zuo Journal of Cybersecurity 3 (1), 55		2021
Searchable Encryption for Conjunctive Queries with Extended Forward and Backward Privacy C Zuo, S Lai, X Yuan, JK Liu, J Shao, H Wang Cryptology ePrint Archive		2021
Verifiable Identity-Based Encryption with Keyword Search for IoT from Lattice L Mei, C Xu, L Xu, X Yu, C Zuo CMC-COMPUTERS MATERIALS & CONTINUA 68 (2), 2299-2314		2021
Attacking the Niederreiter-type cryptosystem based on rank metric C Xu, Y Zhang, L Mei, L Xu, C Zuo International Journal of Embedded Systems 13 (4), 398-404		2020
Enhanced Security for Searchable Symmetric Encryption Supporting Rich Queries C ZUO Monash University		