Dr. Shifeng Sun
Dept of Software Systems & Cybersecurity
**Email:** Shifeng.Sun@monash.edu

## Biography

Shifeng (aka Shi-Feng) Sun is currently a Lecturer in the Faculty of Information Technology at Monash University, Clayton. Prior to joining Monash, Shifeng obtained his PhD in Computer Science from Shanghai Jiao Tong University, China in 2016. His research interest centers on Cryptography and Data Privacy.

## Employment

**Lecturer**
Dept of Software Systems & Cybersecurity
MONASH UNIVERSITY
1 Apr 2020 → present

**Visiting Scientist**
CSIRO Data61
Melbourne, Australia

## Research outputs

**Geometric range search on encrypted data with Forward/Backward security**
Kasra Kermanshahi, S. K., Sun, S-F., Liu, J. K., Steinfeld, R., Nepal, S., Lau, W. F. & Au, M., 23 Mar 2020, (Accepted/In press) In : IEEE Transactions on Dependable and Secure Computing. 18 p.

**Toward forward secure SSE supporting conjunctive keyword search**
Wang, Y., Wang, J., Sun, S., Miao, M. & Chen, X., 27 Sep 2019, In : IEEE Access. 7, p. 142762-142772 11 p.

**Towards multi-user searchable encryption supporting Boolean query and fast decryption**
Wang, Y., Wang, J., Sun, S-F., Liu, J. K., Susilo, W., Baek, J., You, I. & Chen, X., 28 Mar 2019, In : Journal of Universal Computer Science. 25, 3, p. 222-244 23 p.

**Enabling authorized encrypted search for multi-authority medical databases**
Xu, L., Sun, S., Yuan, X., Liu, J. K., Zuo, C. & Chungen, X., 18 Mar 2019, (Accepted/In press) In : IEEE Transactions on Emerging Topics in Computing. 12 p.

**A multi-client DSSE scheme supporting range queries**
Loh, R., Zuo, C., Liu, J. K. & Sun, S. F., 2019, *Information Security and Cryptology : 14th International Conference, Inscrypt 2018 Fuzhou, China, December 14–17, 2018 Revised Selected Papers.* Guo, F., Huang, X. & Yung, M. (eds.). Cham Switzerland: Springer, p. 289-307 19 p. (Lecture Notes in Computer Science ; vol. 11449 ).

**DGM: a dynamic and revocable Group Merkle signature**
Buser, M., Liu, J., Steinfeld, R., Sakzad, A. & Sun, S-F., 2019, *Computer Security - ESORICS 2019: 24th European Symposium on Research in Computer Security Luxembourg, September 23–27, 2019 Proceedings, Part I.* Sako, K., Schneider, S. & Y. A. Ryan, P. (eds.). Cham Switzerland: Springer, p. 194-214 21 p. (Lecture Notes in Computer Science; vol. 11735).

**Dynamic Searchable Symmetric Encryption with forward and stronger backward privacy**
Zuo, C., Sun, S. F., Liu, J. K., Shao, J. & Pieprzyk, J., 2019, *Computer Security – ESORICS 2019 : 24th European Symposium on Research in Computer Security Luxembourg, September 23–27, 2019 Proceedings, Part II.* Sako, K., Schneider, S. & Ryan, P. Y. A. (eds.). Cham Switzerland: Springer, p. 283-303 21 p. (Lecture Notes in Computer Science ;

vol. 11736 ).

**Dynamic searchable symmetric encryption with forward and backward privacy: a survey**
Gan, Q., Zuo, C., Wang, J., Sun, S-F. & Wang, X., 2019, *Network and System Security : 13th International Conference, NSS 2019 Sapporo, Japan, December 15–18, 2019 Proceedings.* Liu, J. K. & Huang, X. (eds.). Cham Switzerland: Springer, p. 37-52 16 p. (Lecture Notes in Computer Science ; vol. 11928 ).

**GraphSE$^2$: an encrypted graph database for privacy-preserving social search**
Lai, S., Yuan, X., Sun, S-F., Liu, J. K., Liu, Y. & Liu, D., 2019, *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security.* Gollmann, D., Kirda, E. & Liang, Z. (eds.). New York NY USA: Association for Computing Machinery (ACM), p. 41-54 14 p.

**Strong leakage and tamper-resilient PKE from refined hash proof system**
Sun, S. F., Gu, D., Au, M. H., Han, S., Yu, Y. & Liu, J., 2019, *Applied Cryptography and Network Security: 17th International Conference, ACNS 2019 Bogota, Colombia, June 5–7, 2019 Proceedings.* Deng, R. H., Gauthier-Umaña, V., Ochoa, M. & Yung, M. (eds.). Cham Switzerland: Springer, p. 486-506 21 p. (Lecture Notes in Computer Science; vol. 11464 ).

**Dynamic searchable symmetric encryption schemes supporting range queries with forward (and backward) security**
Zuo, C., Sun, S. F., Liu, J. K., Shao, J. & Pieprzyk, J., 2018, *Computer Security: 23rd European Symposium on Research in Computer Security, ESORICS 2018 Barcelona, Spain, September 3–7, 2018 Proceedings, Part II.* Lopez, J., Zhou, J. & Soriano, M. (eds.). Cham Switzerland: Springer, p. 228-246 19 p. (Lecture Notes in Computer Science ; vol. 11099 ).

**Practical backward-Secure Searchable Encryption from symmetric puncturable encryption**
Sun, S-F., Yuan, X., Liu, J. K., Steinfeld, R., Sakzad, A., Vo, V. & Nepal, S., 2018, *CCS'18 - Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security: October 15-19, 2018 Toronto, ON, Canada .* Backes, M. & Wang, X. (eds.). New York NY USA: Association for Computing Machinery (ACM), p. 763-780 18 p.

**Result pattern hiding searchable encryption for conjunctive queries**
Lai, S., Patranabis, S., Sakzad, A., Liu, J. K., Mukhopadhyay, D., Steinfeld, R., Sun, S-F., Liu, D. & Zuo, C., 2018, *CCS'18 - Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security: October 15-19, 2018 Toronto, ON, Canada.* Backes, M. & Wang, X. (eds.). New York NY USA: Association for Computing Machinery (ACM), p. 745-762 18 p.

**Towards efficient verifiable conjunctive keyword search for large encrypted database**
Wang, J., Chen, X., Sun, S-F., Liu, J. K., Au, M. H. & Zhan, Z-H., 2018, *Computer Security: 23rd European Symposium on Research in Computer Security, ESORICS 2018 Barcelona, Spain, September 3–7, 2018 Proceedings, Part II.* Lopez, J., Zhou, J. & Soriano, M. (eds.). Cham Switzerland: Springer, p. 83-100 18 p. (Lecture Notes in Computer Science ; vol. 11099 ).

**Public key encryption resilient to leakage and tampering attacks**
Sun, S-F., Gu, D., Parampalli, U., Yu, Y. & Qin, B., 1 Nov 2017, In : Journal of Computer and System Sciences. 89, p. 142-156 15 p.

**Related-key secure key encapsulation from extended computational bilinear Diffie–Hellman**
Qin, B., Liu, S., Sun, S., Deng, R. H. & Gu, D., 1 Sep 2017, In : Information Sciences. 406-407, p. 1-11 11 p.

**RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero**
Sun, S-F., Au, M. H., Liu, J. K. & Yuen, T. H., 2017, *Computer Security – ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Proceedings.* Foley, S., Snekkenes, E. & Gollmann, D. (eds.). Cham, Switzerland: Springer, Vol. 10493 . p. 456-474 19 p. (Lecture Notes in Computer Science; vol. 10493 ).

**Towards multi-user searchable encryption supporting boolean query and fast decryption**
Wang, Y., Wang, J., Sun, S-F., Liu, J. K., Susilo, W. & Chen, X., 2017, *Provable Security: 11th International Conference, ProvSec 2017, 2017, Xi'an, China, October 23-25, 2017.* Okamoto, T., Yu, Y., Ao, M. H. & Li, Y. (eds.). Cham Switzerland: Springer, Vol. 10592 . p. 24-38 15 p. (Lecture Notes in Computer Science ; vol. 10592 ).

**Public key cryptosystems secure against memory leakage attacks**
Sun, S-F., Han, S., Gu, D. & Liu, S., 1 Nov 2016, In : IET Information Security. 10, 6, p. 403-412 10 p.

**Privacy-preserving data sharing scheme over cloud for social applications**
Lyu, C., Sun, S-F., Zhang, Y., Pande, A., Lu, H. & Gu, D., 1 Oct 2016, In : Journal of Network and Computer Applications. 74, p. 44-55 12 p.

**An efficient non-interactive multi-client searchable encryption with support for boolean queries**
Sun, S-F., Liu, J. K., Sakzad, A., Steinfeld, R. & Yuen, T. H., 15 Sep 2016, *Computer Security - ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26–30, 2016, Proceedings, Part I.* Askoxylakis, I., Ioannidis, S., Katsikas, S. & Meadows, C. (eds.). Switzerland: Springer, p. 154-172 19 p. (Lecture Notes in Computer Science ; vol. 9878 ).

**Efficient chosen ciphertext secure identity-based encryption against key leakage attacks**
Sun, S-F., Gu, D. & Liu, S., 25 Jul 2016, In : Security and Communication Networks. 9, 11, p. 1417-1434 18 p.

**Efficient construction of completely non-malleable CCA secure public key encryption**
Sun, S. F., Gu, D., Liu, J. K., Parampalli, U. & Yuen, T. H., 30 May 2016, *ASIA CCS 2016 - Proceedings of the 11th ACM Asia Conference on Computer and Communications Security.* Wang, X. & Huang, X. (eds.). New York NY USA: Association for Computing Machinery (ACM), p. 901-906 6 p.

**Anonymizing bitcoin transaction**
Wijaya, D. A., Liu, J. K., Steinfeld, R., Sun, S. F. & Huang, X., 2016, *Information Security Practice and Experience : 12th International Conference, ISPEC 2016, Zhangjiajie, China, November 16–18, 2016, Proceedings.* Bao, F., Chen, L., Deng, R. H. & Wang, G. (eds.). Cham, Switzerland: Springer, p. 271-283 13 p. (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); vol. 10060 ).

**Efficient completely non-malleable and RKA secure public key encryptions**
Sun, S-F., Parampalli, U., Yuen, T. H., Yu, Y. & Gu, D., 2016, *Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II.* Liu, J. K. & Steinfeld, R. (eds.). Switzerland: Springer, p. 134-150 17 p. (Lecture Notes in Computer Science; vol. 9723).

**RKA-secure public key encryptions against efficiently invertible functions**
Sun, S-F., Liu, J. K., Yu, Y., Qin, B. & Gu, D., 2016, In : Computer Journal. 59, 11, p. 1637-1658 22 p.

**Fully secure wicked identity-based encryption against key leakage attacks**
Sun, S-F., Gu, D. & Huang, Z., Oct 2015, In : Computer Journal. 58, 10, p. 2520-2536 17 p.

**SGOR: secure and scalable geographic opportunistic routing with received signal strength in WSNs**
Lyu, C., Gu, D., Zhang, X., Sun, S., Zhang, Y. & Pande, A., 15 Mar 2015, In : Computer Communications. 59, p. 37-51 15 p.

**Towards efficient, secure, and fine-grained access control system in MSNs with flexible revocations**
Sun, S-F., Lyu, C., Gu, D., Zhang, Y. & Ren, Y., 2015, In : International Journal of Distributed Sensor Networks. 2015, 15 p., 857405.

**Efficient leakage-resilient identity-based encryption with CCA security**
Sun, S-F., Gu, D. & Liu, S., 2014, *Pairing-Based Cryptography – Pairing 2013: 6th International Conference Beijing, China, November 22-24, 2013 Revised Selected Papers.* Cao, Z. & Zhang, F. (eds.). Cham Switzerland: Springer, p. 149-167 19 p. (Lecture Notes in Computer Science; vol. 8365).

**Efficient, fast and scalable authentication for VANETs**
Lyu, C., Gu, D., Zhang, X., Sun, S. & Tang, Y., 2013, *2013 IEEE Wireless Communications and Networking Conference (WCNC).* Wang, J. (ed.). Piscataway NJ USA: IEEE, Institute of Electrical and Electronics Engineers, p. 1768-1773 6 p. 6554831