Haiyang XUE

School of Computing and Information Systems
Singapore Management University (SMU)
80 Stamford Road
Singapore 178902

Email: haiyangxue@smu.edu.sg

Education

PhD, The Chinese Academy of Sciences, China, 2015
Master of Science, Shandong University, China, 2012
Bachelor of Science, Shandong University, China, 2009

Academic Appointments

Assistant Professor of Computer Science, School of Computing and Information Systems, SMU, Jul 2024 – present
Research Assistant Professor, Department of Computing, The Hong Kong Polytechnic University, Dec 2022 – Jun 2024
Research Assistant Professor, Department of Computer Science, The University of Hong Kong, Jan 2022 – Nov 2022

Awards and Honors

Merit Prize in the "Fintech-Cryptography" competition, People's Bank of China and Tsinghua University, 2022
First Prize in the PQC, held by the Chinese Association for Cryptologic Research (CACR), 2020
Two Second Prizes in the PQC competition, held by CACR, 2020
Best Paper Award, IWSEC 2015
Best Paper Award, ProvSec 2014

RESEARCH

Publications

<u>Journal Articles [Refereed]</u>

Efficient Verifiably Encrypted ECDSA Schemes from Castagnos-Laguillaumie and Joye-Libert Encryptions, by YANG, Xiao; ZHANG, Chengru; XUE, Haiyang; AU, Man Ho. (2024) *IEEE Transactions on Information Forensics and Security*, 19, 4161-4173, 2024. http://dx.doi.org/10.1109/TIFS.2024.3375622 (Published)

P^{2}FRPSI: Privacy-Preserving Feature Retrieved Private Set Intersection, by LING, Guowei; TANG, Fei; CAI Chaochao; SHAN, Jinyong; XUE, Haiyang; LI, Wulu; TANG, Peng; HUANG, Xinyi; QIU Weidong. (2024) *IEEE Transactions on Information Forensics and Security*, 19, 2201-2216, 2024. https://doi.org/10.1109/TIFS.2023.3343973 (Published)

Analysis of blockchain protocol against static adversarial miners corrupted by long delay attackers, by YUAN, Quan; WEI, Puwen; JIA, Keting; XUE, Haiyang. (2020) *Science China Information Sciences*, 63, 1-15, 2020.

https://doi.org/10.1007/s11432-019-9916-5 (Published)

Regular lossy functions and their applications in leakage-resilient cryptography, by CHEN, Yu; QIN, Baodong; XUE, Haiyang. (2018) *Theoretical Computer Science*, 739, 13-38, 2018. https://doi.org/10.1016/j.tcs.2018.04.043 (Published)

Fault attacks on hyperelliptic curve discrete logarithm problem over binary field, by WANG, Mingqiang; XUE, Haiyang; ZHAN, Tao. (2014) *Science China Information Sciences*, 57, 1-17, 2014. https://doi.org/10.1007/s11432-013-5048-6 (Published)

Conference Proceedings

Efficient Zero-Knowledge Arguments For Paillier Cryptosystem, by GONG Borui; LAU, Wang Fat; YANG, Rupeng; XUE, Haiyang; LI, Lichun. *IEEE S&P 2024: Proceedings of 45th IEEE Symposium on Security and Privacy, San Francisco, CA, USA, May 20-22, 2024*. https://doi.ieeecomputersociety.org/10.1109/SP54263.2024.00093 (Published)

Efficient Multiplicative-to-Additive Function from Joye-Libert Cryptosystem and Its Application to Threshold ECDSA, by XUE, Haiyang; AU, Man Ho; LIU Mengling; CHAN, Kwan Yin; CUI, Handong; XIE, Xiang; YUEN, Tsz Hon; ZHANG, Chengru. *ACM CCS 2023: Proceedings of the 30th ACM Conference on Computer and Communications Security, Copenhagen, Denmark, Nov 26-30, 2023,* (pp. 2974-2988). https://doi.org/10.1145/3576915.3616595 (Published)

Resumable ZeroKnowledge for Circuits from Symmetric Key Primitives, by ZHANG, Handong; WEI, Puwen; XUE, Haiyang; DENG, Yi; LI, Jinsong; WANG, Wei; LIU, Guoxiao. *ACISP 2022: Proceeding of 27th Australasian Conference on Information Security and Privacy, Wollongong, Australia, Nov 28-30, 2022,* (pp. 375-398). https://doi.org/10.1007/978-3-031-22301-3_19 (Published)

Efficient Online-friendly Two-Party ECDSA Signature, by XUE, Haiyang; AU, Man Ho; XIE, Xiang; YUEN, Tsz Hon; CUI, Handong. *ACM CCS 2021: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Nov 15-19, 2021,* (pp. 558-573). https://dl.acm.org/doi/proceedings/10.1145/346012 (Published)

Strongly Secure Authenticated Key Exchange from Supersingular Isogenies, by XU, Xiu; XUE, Haiyang; WANG, Kunpeng; AU, Man Ho; TIAN, Song. *ASIACRYPT (1) 2019: Proceeding of 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, Dec 8-12, 2019,* (pp. 278-308). https://doi.org/10.1007/978-3-030-34578-5_11 (Published)

Tighter Security Proofs for Post-quantum Key Encapsulation Mechanism in the Multi-challenge Setting, by ZHANG, Zhengyu, WEI, Puwen; XUE, Haiyang. *CANS 2019: Proceeding of 18th International Conference on Cryptology and Network Security, Fuzhou, China, Oct 25-27, 2019,* (pp. 141-160). https://doi.org/10.1007/978-3-030-31578-8_8 (Published)

Constructing Strong Designated Verifier Signatures from Key Encapsulation Mechanisms, by GONG Borui; AU, Man Ho; XUE, Haiyang. *TrustCom/BigDataSE 2019: Proceeding of 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ Proceeding of 13th IEEE International Conference on Big Data Science and Engineering, Rotorua, New Zealand, Aug 5-8, 2019,* (pp. 586-593). https://doi.org/10.1109/TrustCom/BigDataSE.2019.00084 (Published)

Understanding and Constructing AKE via Double-Key Key Encapsulation Mechanism, by XUE, Haiyang; LU, Xianhui; LI, Bao; LIANG, Bei; HE, Jingnan. *ASIACRYPT (2) 2018: Proceeding of 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, Australia, Dec 2-6, 2018,* (pp. 158-189). https://doi.org/10.1007/978-3-030-03329-3_6 (Published)

Regularly Lossy Functions and Applications, by CHEN, Yu; QIN, Baodong; XUE, Haiyang. *CT-RSA 2018: Proceeding of the Cryptographers' Track at the RSA Conference 2018, San Francisco, USA, Apr 16-20, 2018,* (pp. 491-511). https://doi.org/10.1007/978-3-319-76953-0 (Published)

Preprocess-then-NTT Technique and Its Applications to Kyber and NewHope, by ZHOU, Shuai; XUE, Haiyang; ZHANG, Daode; WANG, Kunpeng; LU, Xianhui; LI, Bao; HE, Jingnan. *Inscrypt 2018: Proceeding of 14th International Conference on Information Security and Cryptology, Fuzhou, China, Dec 14-17, 2018,* (pp. 117-137). https://doi.org/10.1007/978-3-030-14234-6_7 (Published)

Lattice-Based Dual Receiver Encryption and More, by ZHANG, Daode; ZHANG, Kai; LI, Bao; LU, Xianhui; XUE, Haiyang; LI, Jie. *ACISP 2018: Proceeding of 23th Australasian Conference on Information Security and Privacy, Wollongong, NSW, Australia, Jul 11-13, 2018,* (pp. 520-538). https://doi.org/10.1007/978-3-319-93638-3_30 (Published)

Towards Tightly Secure Deterministic Public Key Encryption, by ZHANG, Daode; LI, Bao; LIU, Yamin; XUE, Haiyang; LU, Xianhui; JIA, Dingding. *ICICS 2017: Proceeding of 19th International Conference on Information and Communications Security, Beijing, China, Dec 6-8, 2017,* (pp. 154-161). https://doi.org/10.1007/978-3-319-89500-0_13 (Published)

Lossy Projective Hashing and Its Applications, by XUE, Haiyang; LIU, Yamin, LU, Xianhui; LI, Bao. *INDOCRYPT 2015:*

Proceeding of 16th International Conference on Cryptology in India, Bangalore, India, Dec 6-9, 2015, (pp. 64-84). https://doi.org/10.1007/978-3-319-26617-6_4 (Published)

Identity-Based Lossy Encryption from Learning with Errors, by HE, Jingnan, LI, Bao; LU, Xianhui, JIA, Dingding; XUE, Haiyang; SUN, Xiaochao. *IWSEC 2015: Proceeding of 10th International Workshop on Security, Nara, Japan, Aug 26-28, 2015,* (pp 3-20). https://doi.org/10.1007/978-3-319-22425-1_1 (Published, Best Paper Award)

On the Lossiness of 2k -th Power and the Instantiability of Rabin-OAEP, by XUE, Haiyang; LI, Bao; LU, Xianhui; WANG, Kunpeng; LIU, Yamin. *CANS 2014: Proceeding of 13th International Conference on Cryptology and Network Security, Heraklion, Crete, Greece, Oct 22-24, 2014,* (pp. 34-49). https://doi.org/10.1007/978-3-319-12280-9_3 (Published)

Lossy Trapdoor Relation and Its Applications to Lossy Encryption and Adaptive Trapdoor Relation, by XUE, Haiyang; LU, Xianhui; LI, Bao; LIU, Yamin. *ProvSec 2014: Proceeding of 8th International Conference on Provable Security, Hong Kong, China, Oct 9-10, 2014,* (pp.162-177). https://doi.org/10.1007/978-3-319-12475-9_12 (Published, Best Paper Award)

Efficient Lossy Trapdoor Functions Based on Subgroup Membership Assumptions, by XUE, Haiyang; LI, Bao; LU, Xianhui; JIA, Dingding; LIU, Yamin. *CANS 2013: Proceeding of 12th International Conference on Cryptology and Network Security, Paraty, Brazil, Nov 20-22, 2013,* (pp. 235-250). https://doi.org/10.1007/978-3-319-02937-5_13 (Published)

TEACHING

Courses Taught

<u>Singapore Management University</u>

Undergraduate Programmes :

Postgraduate Professional Programmes :

EXTERNAL SERVICE – PROFESSIONAL

Committee Member, 18th International Conference on Provable and Practical Security (ProvSec 2024)

Committee Member, 4th International Conference on Emerging Information Security and Applications (EISA 2023)

Committee Member, 19th International Conference on Information Security and Cryptology (Inscrypt 2023)

Committee Member, 17th International Conference on Provable and Practical Security (ProvSec 2023)

Committee Member, 18th International Conference on Information Security Practice and Experience (ISPEC 2023)

Committee Member, 16th International Conference on Provable and Practical Security (ProvSec 2022)

Committee Member, 15th International Conference on Provable and Practical Security (ProvSec 2021)

Committee Member, 14th International Conference on Provable and Practical Security (ProvSec 2020)