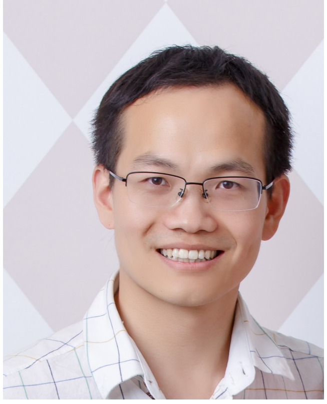
XUE, Haiyang

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

Email: haiyangxue@smu.edu.sg



Education

PhD, 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

Research Interests

I am broadly interested in cryptography and its applications in cybersecurity, including but not limited to post-quantum cryptography, threshold cryptography, privacy-enhancing technologies, such as zero-knowledge proof, multiparty computing, etc. I aim to bridge the gap between theoretical cryptography and practical security issues by developing innovative cryptographic solutions.

Publications

Journal Articles [Refereed]

Novel secure outsourcing of modular inversion for arbitrary and variable modulus, by TIAN, Chengliang; YU, Jia; ZHANG, Hanlin; XUE, Haiyang; WANG, Cong; REN, Kui. (2022). *IEEE Transactions on Services Computing, 15* (1), 241-253. https://doi.org/10.1109/tsc.2019.2937486 (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* (3), 1-15. https://doi.org/10.1007/s11432-019-9916-5 (Published)

Deterministic identity-based encryption from lattice-based programmable hash functions with high min-entropy, by ZHANG, Daode; LI, Jie; LI, Bao; LU, Xianhui; XUE, Haiyang; JIA, Dingding; LIU, Yamin. (2019). *Security and Communication Networks, 2019* 1-12. https://doi.org/10.1155/2019/1816393 (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. 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* (3), 1-17. https://doi.org/10.1007/s11432-013-5048-6 (Published)

Journal Articles [Non-Refereed]

Efficient verifiably encrypted ECDSA schemes from Castagnos-Laguillaumie and Joye-Libert encryptions, by YANG, Xiao; ZHANG, Chengru; XUE, Haiyang; AU, Ho Man. (2024). *IEEE Transactions on Information Forensics and Security, 19* 4161-4173. https://doi.org/10.1109/tifs.2024.3375622 (Published)

P²FRPSI: 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. https://doi.org/10.1109/tifs.2023.3343973 (Published)

Conference Proceedings

Efficient multiplicative-to-additive function from Joye-Libert cryptosystem and its application to threshold ECDSA, by XUE, Haiyang; AU, Ho Man; LIU, Mengling; CHAN, Yin Kwan; CUI, Handong; XIE, Xiang; YUEN, Hon Tsz; ZHANG, Chengru. (2023.0). *CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, Denmark, November 26-30,* (pp. 2974-2988) New York: ACM. https://doi.org/10.1145/3576915.3616595 (Published)

On the lossiness of 2k-th power and the instantiability of Rabin-OAEP, by XUE, Haiyang; LI, Bao; LU, Xianhui; WANG, Kunpeng; LIU, Yamin. (2014.0). *Proceedings of the 13th International Conference on Cryptology and Network Security, CANS 2014, Crete, Greece, October 22-24,* (pp. 34-49) Cham: Springer. https://doi.org/10.1007/978-3-319-12280-9_3 (Published)

Direct range proofs for Paillier cryptosystem and their applications, by XIE, Zhikang; LIU, Mengling; XUE, Haiyang; AU, Man Ho; DENG, Robert H.; YIU, Siu-Ming. (2024.0). *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2024) : Salt Lake City, USA, October 14-18,* Salt Lake City, USA: ACM Digital Library. (Published)

Efficient zero-knowledge arguments for Paillier cryptosystem, by GONG, Borui; LAU, Wang Fat; AU, Man Ho; YANG, Rupeng; XUE, Haiyang; LI, Lichun. (2024.0). *Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, May 19-23,* (pp. 1-19) Los Alamitos, CA, USA: IEEE. (Published)

Resumable zero-knowledge for circuits from symmetric key primitives, by ZHANG, Handong; WEI, Puwen; XUE, Haiyang; DENG, Yi; LI, Jinsong; WANG, Wei; LIU, Guoxiao. (2022.0). *Proceedings of the 27th Australasian Conference, ACISP 2022 Wollongong, Australia, November 28-30,* (pp. 375-398) Cham: Springer. https://doi.org/10.1007/978-3-031-22301-3_19 (Published)

Efficient online-friendly two-party ECDSA signature, by XUE, Haiyang; AU, Ho Man; XIE, Xiang; YUEN, Hon Tsz; CUI, Handong. (2021.0). *CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Conference, November 15-19,* (pp. 558-573) New York: ACM. https://doi.org/10.1145/3460120.3484803 (Published)

Strongly secure authenticated key exchange from supersingular isogenies, by XU, Xiu; XUE, Haiyang; WANG, Kunpeng; AU, Ho Man; TIAN, Song. (2019.0). *Proceedings of the 25th International Conference on the Theory and Application of Cryptology and Information Security Kobe, Japan, 2019 December 8-12,* (pp. 278-308) Cham: Springer. 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. (2019.0). *Proceedings of the 18th International Conference, CANS 2019, Fuzhou, China, October 25–27,* (pp. 141-160) Cham: Springer. 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, Ho Man; XUE, Haiyang. (2019.0). *Proceedings of the 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, August 5-8,* (pp. 586-593) Los

Alamitos, CA: IEEE. https://doi.org/10.1109/trustcom/bigdatase.2019.00084 (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. (2019.0). *Proceedings of the 14th International Conference, Inscrypt 2018, Fuzhou, China, December 14-17,* (pp. 117-137) Cham: Springer. https://doi.org/10.1007/978-3-030-14234-6_7 (Published)

Understanding and constructing AKE via double-key key encapsulation mechanism, by XUE, Haiyang; LU, Xianhui; LI, Bao; LIANG, Bei; HE, Jingnan. (2018.0). *Proceedings of the 24th International Conference on the Theory and Application of Cryptology and Information Security Brisbane, Australia, December 2-6,* (pp. 158-189) Cham: Springer. https://doi.org/10.1007/978-3-030-03329-3_6 (Published)

Lattice-based dual receiver encryption and more, by ZHANG, Daode; ZHANG, Kai; LI, Bao; LU, Xianhui; XUE, Haiyang; LI, Jie. (2018.0). *Proceedings of the 23rd Australasian Conference, ACISP 2018 Wollongong, Australia, July 11-13,* (pp. 520-538) Cham: Springer. https://doi.org/10.1007/978-3-319-93638-3_30 (Published)

Regularly lossy functions and applications, by CHEN, Yu; QIN, Baodong; XUE, Haiyang. (2018.0). *Proceedings of the Cryptographers' Track at the RSA Conference 2018 San Francisco, CA, April 16-20,* (pp. 491-511) Cham: Springer. https://doi.org/10.1007/978-3-319-76953-0_26 (Published)

Towards tightly secure deterministic public key encryption, by ZHANG, Daode; LI, Bao; LIU, Yamin; XUE, Haiyang; LU, Xianhui; JIA, Dingding. (2018.0). *Proceedings of the 19th International Conference, ICICS 2017 Beijing, China, December 6-8,* (pp. 154-161) Cham: Springer. https://doi.org/10.1007/978-3-319-89500-0_13 (Published)

Compact hierarchical IBE from lattices in the standard model, by ZHANG, Daode; FANG, Fuyang; LI, Bao; XUE, Haiyang; LIANG, Bei. (2018.0). *Proceedings of the19th International Conference, ICICS 2017, Beijing, China, December 6-8,* (pp. 210-221) Cham: Springer. https://doi.org/10.1007/978-3-319-89500-0_19 (Published)

New framework of password-based authenticated key exchange from only-one lossy encryption, by XUE, Haiyang; LI, Bao; HE, Jingnan. (2017.0). *Proceedings of the 11th International Conference, ProvSec 2017, Xi'an, China, October 23-25,* (pp. 188-198) Cham: Springer. https://doi.org/10.1007/978-3-319-68637-0_11 (Published)

IND-PCA secure KEM is enough for password-based authenticated key exchange (short paper), by XUE, Haiyang; LI, Bao; LU, Xianhui. (2017.0). *Proceedings of the 12th International Workshop on Security, IWSEC 2017 Hiroshima, Japan, August 30 - September 1,* (pp. 231-241) Cham: Springer. https://doi.org/10.1007/978-3-319-64200-0_14 (Published)

Lossy key encapsulation mechanism and its applications, by LIU, Yamin; LU, Xianhui; LI, Bao; XUE, Haiyang. (2016.0). *Proceedings of the 19th International Conference Seoul, South Korea, 2016 November 30 - December 2,* (pp. 126-144) Cham: Springer. (Published)

(Deterministic) hierarchical identity-based encryption from learning with rounding over small modulus, by FANG, Fuyang; LI, Bao; LU, Xianhui; LIU, Yamin; JIA, Dingding; XUE, Haiyang. (2016.0). *ASIA CCS '16: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, May 30 - June 3,* (pp. 907-912) New York: ACM. https://doi.org/10.1145/2897845.2897922 (Published)

Lossy projective hashing and its applications, by XUE, Haiyang; LIU, Yamin; LU, Xianhui; LI, Bao. (2015.0). *Proceedings of the 16th International Conference on Cryptology in India, Bangalore, India, 2015 December 6-9,* (pp. 64-84) Cham: Springer. 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. (2015.0). *Proceedings of the 10th International Workshop on Security, IWSEC 2015 Nara, Japan, August 26-28, ,* (pp. 3-20) Cham: Springer. https://doi.org/10.1007/978-3-319-22425-1_1 (Published)

Lossy trapdoor relation and its applications to lossy encryption and adaptive trapdoor relation, by XUE, Haiyang; LU, Xianhui; LI, Bao; LIU, Yamin. (2014.0). *Proceedings of the 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10,* (pp. 162-177) Cham: Springer. https://doi.org/10.1007/978-3-319-12475-9_12 (Published)

Efficient lossy trapdoor functions based on subgroup membership assumptions, by XUE, Haiyang; LI, Bao;

LU, Xianhui; JIA, Dingding; LIU, Yamin. (2013.0). *Proceedings of the 12th International Conference, CANS 2013, Paraty, Brazil, November 20-22,* (pp. 235-250) Cham: Springer. https://doi.org/10.1007/978-3-319-02937-5_13 (Published)

Research Grants

<u>Singapore Management University</u>

Threshold Digital Signatures for Blockchain-based Cryptocurrency, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): XUE, Haiyang, 2024, S$120,000

TEACHING

Courses Taught

<u>Singapore Management University</u>

Undergraduate Programmes :

Foundations of Cybersecurity

EXTERNAL SERVICE – PROFESSIONAL

Committee Member, ACM CCS 2025, 2024 - Present

Committee Member, Inscrypt 2024, 2024

Committee Member, ProvSec 2024, 2024