Haiyang Xue (薛海洋)

Email: haiyangxc@gmail.com **Mobile Phone:** 57631077

Address: Rm 207 Chow Yei Ching Building, The University of Hong Kong, Pokfulam, Hong Kong

Homepage: https://haiyangxc.github.io/hyxue/

Education

2012-2015 PhD, Chinese Academy of Sciences, "Lossy Trapdoor Related Primitives and Their Applications in Public Key Encryption" under the supervision of Bao Li.

2009-2012 Master in Information Security, Shandong University

2005-2009 Bachelor in Mathematics, Shandong University

Experiences

July 2015 – Oct 2018 State Key Lab of Information Security, IIE, CAS, *Cryptography Researcher*

Oct 2018 – Jan 2020 Joint Lab. on Blockchain of PolyU and Monash, PolyU, *Post-doctoral Fellow*

Feb 2020 – present The Hong Kong University, *Post-doctoral Fellow*

Post-Quantum Cryptography Algorithms

- ✓ **LAC：La**ttice-based **C**ryptosystem
  - Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, Kunpeng Wang
  - Round 2 Candidate for NIST Post-Quantum Cryptography Standardization
  - First prize of Chinese post-quantum cryptography competition
- ✓ **SIAKE: S**upersingular **I**sogeny based **A**uthenticated **K**ey **E**xchange
  - Haiyang Xue, Xianhui Lu, Kunpeng Wang, Song Tian, Xiu Xu, Jingnan He, Bao Li
  - Second prize of Chinese post-quantum cryptography competition

Publications

[1] Quan Yuan, Puwen Wei, Keting Jia, **Haiyang Xue**: Analysis of blockchain protocol against static adversarial miners corrupted by long delay attackers. *Sci. China Inf. Sci*. 63(3) (2020)

[2] Xiu Xu, **Haiyang Xue***, Kunpeng Wang, Man Ho Au, Song Tian: Strongly Secure Authenticated Key Exchange from Supersingular Isogenies, *ASIACRYPT 2019*, pp. 278-308.

[3] **Haiyang Xue,** Xianhui Lu, Bao Li, Jingnan He: Understanding and Constructing Authenticated Key Exchange via Double Key Key Encapsulated Mechanism, *ASIACRYPT 2018*, pp. 158-189

[4] Daode Zhang, Jie Li, Bao Li, Xianhui Lu, **Haiyang Xue***, Dingding Jia, Yamin Liu: Deterministic Identity-Based Encryption from Lattice-Based Programmable Hash Functions with High Min-Entropy, *SCN*, pp. 1-12.

[5] Yu Chen, Baodong Qin, **Haiyang Xue***: Regularly Lossy Functions and Their Applications, *CT-RSA* 2018, pp 491-511.

Haiyang Xue (薛海洋)

[6] Yu Chen, Baodong Qin, **Haiyang Xue**: Regular lossy functions and their applications in leakage-resilient cryptography. *Theor. Comput. Sci.* 739, pp. 13-38.

[7] Shuai Zhou, **Haiyang Xue**, Daode Zhang, Kunpeng Wang, Xianhui Lu, Bao Li, Jingnan He:Preprocess-then-NTT Technique and Its Applications to Kyber and NewHope. *Inscrypt 2018*, 117-137.

[8] **Haiyang Xue**, Bao Li, Xianhui Lu: IND-PCA Secure KEM Is Enough for Password-Based Authenticated Key Exchange, *IWSEC 2017*, 231-241.

[9] Daode Zhang, Bao Li, Yamin Liu, **Haiyang Xue**, Xianhui Lu and Dingding Jia. Towards Tightly Secure Deterministic Public Key Encryption. *ICICS 2017*.

[10] Fuyang Fang, Bao Li, Xianhui Lu, Yamin Liu, Dingding Jia, **Haiyang Xue**: (Deterministic) Hierarchical Identity-based Encryption from Learning with Rounding over Small Modulus. *AsiaCCS 2016*, 907-912.

[11] **Haiyang Xue**, Yamin Liu, Xianhui Lu, Bao Li: Lossy Projective Hashing and Its Applications. *INDOCRYPT 2015*, 64-84.

[12] Jingnan He, Bao Li, Xianhui Lu, Dingding Jia, **Haiyang Xue**, Xiaochao Sun: Identity-Based Lossy Encryption from Learning with Errors. *IWSEC 2015*, 3-20 (**Best Paper**)

[13] **Haiyang Xue**, Bao Li, Xianhui Lu, Kunpeng Wang, Yamin Liu: On the Lossiness of 2*k*-th Power and the Instantiability of Rabin-OAEP. *CANS 2014*, 34-49.

[14] **Haiyang Xue**, Xianhui Lu, Bao Li, Yamin Liu: Lossy Trapdoor Relation and Its Applications to Lossy Encryption and Adaptive Trapdoor Relation. *ProvSec 2014*, 162-177 (**Best Paper**)

[15] Mingqiang Wang, **Haiyang Xue**, Tao Zhan: Fault attacks on hyper-elliptic curve discrete logarithm problem over binary field. *SCIENCE CHINA Information Sciences 57(3)*: 1-17 (2014)

[16] **Haiyang Xue**, Bao Li, Xianhui Lu, Dingding Jia, Yamin Liu: Efficient Lossy Trapdoor Functions Based on Subgroup Membership Assumptions. *CANS 2013*: 235-250.

Awards

First prize of Chinese post-quantum cryptography competition (LAC.PKE)
Second prizes of Chinese post-quantum cryptography competition (SIAKE, and LAC.KEX)
Best Paper Award IWSEC 2015
Best Paper Award ProvSec 2014

Funding

1. Climbing Program, 2019-2021, Post-quantum Secure Authenticated Key Exchange (RMB 300,000)
2. Science and Technology Major Project of Beijing Municipal Commission of Education, Co-PI, 2019-2020, Quantum-resistant public key cryptosystems (RMB 3,000,000)
3. National Natural Science Foundation of China (NSFC), 2017-2019, Lossy Trapdoor Technique and Its Applications to Public Key Cryptography (RMB 200,000)
4. National Cryptography Development Fund, 2017-2019, Basic Tools of Provable Security in Cryptography (RMB 100,000)