Haiyang Xue (薛海洋)

Email: haiyangxc@gmail.com **Mobile Phone:** 57631077
Address: No. 99 Baker Street, Hung Hom, Hong Kong

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

Post-Quantum Cryptography Algorithms

✓ **LAC**: Round 2 Candidate Algorithm for NIST Post-Quantum Cryptography Standardization

Co-Designer (4/10) of **LAC** for NIST Post-Quantum Cryptography Standardization. My main contributions are the security analysis and proof of KEM and Authenticated-KE algorithms.

✓ National Cryptographic Algorithm Competition by Chinese Association of Cryptologic Research

SIAKE	Primary designer (1/7)	Super-singular Isogeny-based AKE	**Second Prize**
LAC.PKE	Co-Designer (4/10)	Lattice-based PKE	**First Price**
LAC.KE	Co-Designer (4/10)	Lattice-based AKE	**Second Price**

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.

[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 2k-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

Best Paper Award ProvSec 2014;   Best Paper Award IWSEC 2015

First Price and Second Price in National Cryptographic Algorithm Competition 2019

Funding

1. National Natural Science Foundation of China (NSFC) 2017-2019, Lossy Trapdoor Technique and Its Applications to Public Key Cryptography.
2. National Cryptography Development Fund 2017-2019, Basic Tools of Provable Security in Cryptography