# Haiyang Xue

Email: haiyangxc@gmail.com      Homepage: https://haiyangxc.github.io/hyxue/

## Curriculum Vitae

Department of Computer Sciences, The University of Hong Kong.
Room 207, Chow Yei Ching Building, The University of Hong Kong, Pokfulam, Hong Kong
Phone: +85257631077
Email: haiyangxc@gmail.com
Homepage: https://haiyangxc.github.io/hyxue/

## Research Interests

Theory and applications of cryptography; Post-quantum cryptography, especially authenticated key exchange from lattice and isogeny; Multiparty computation; Zero-knowledge proof.

## Education

PhD, Institute of Information Engineering, Chinese Academy of Sciences, 2015
Thesis: Lossy Trapdoor and Their Applications in Public Key Encryption, Supervisor: Bao Li

Master in Information Security, School of Mathematics, Shandong University, 2012

Bachelor in Mathematics, School of Mathematics, Shandong University, 2009

## Working Experience

| | |
|---|---|
| Jan. 2022 -current | Research Assistant Professor<br>The University of Hong Kong |
| July 2015 -Nov.2021 | Lecturer<br>Institute of Information Engineering, Chinese Academy of Sciences |
| Sep. 2020 -Sep.2021 | Research Associate<br>The University of Hong Kong, hosted by Associate Professor Man Ho Au |
| Oct.2018 - Sep.2020 | Post-doctoral Fellow (Oct.2018-Oct.2019) / Research Fellow (Oct.2019- Sep.2020)<br>The Hong Kong Polytechnic University, hosted by Associate Professor Man Ho Au |

## Highlights

| | |
|---|---|
| Post-quantum Algorithms | LAC: Lattice-based Cryptosystem<br>2nd round candidate of NIST post-quantum standardization process<br>First prize of Chinese post-quantum cryptography competition<br>SIAKE: Supersingular Isogeny based Authenticated Key Exchange<br>Second prize of Chinese post-quantum cryptography competition |
| Publications | 15+ peer-reviewed papers at CCS 2021, ASIACRYPT 2019, ASIACRYPT 2018, CT-RSA 2018, Theoretical Computer Science, etc. |

# Haiyang Xue

Email: haiyangxc@gmail.com Homepage: https://haiyangxc.github.io/hyxue/

## Selected Works

- ***Haiyang Xue**, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui:* Efficient Online-friendly Two-Party ECDSA Signature. The 28th ACM Conference on Computer and Communications Security (ACM CCS 2021). (to appear)
  We propose an online-friendly two-party ECDSA with a lightweight online phase and a single multiplicative-to-additive function in the offline phase.

- ***Haiyang Xue**, Xianhui Lu, Kunpeng Wang, Song Tian, Xiu Xu, Jingnan He, Bao Li:* SIAKE: Supersingular Isogeny based Authenticated Key Exchange, Technical Report.
  It won the second prize in the Chinese post-quantum cryptography competition. This is the follow-up work of our paper in Asiacrypt 2019, with additional security analysis in the Quantum Random Oracle Model.

- *Xiu Xu, **Haiyang Xue**, Kunpeng Wang, Man Ho Au, Song Tian:* Strongly Secure Authenticated Key Exchange from Supersingular Isogenies. The 25th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2019), pages 178-308 (2019). Acceptance Rate: 23.1%
  We propose a strongly secure authenticated key exchange from supersingular isogenies in the random oracle model. It solves an open problem given by Steven Galbraith.

- ***Haiyang Xue**, Xianhui Lu, Bao Li, Bei Liang, Jingnan He:* Understanding and Constructing AKE via Double-key Key Encapsulation Mechanism. The 24th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018), pages 158-189 (2018). Acceptance Rate: 27.7%
  We give a unified framework for constructing implicitly authenticated key exchange. Our framework captures celebrated works including HMQC, NAXOS.

- *Xianhui Lu, Yamin Liu, Dingding Jia, **Haiyang Xue**, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, Kunpeng Wang* LAC: Lattice-based Cryptosystem, Technical Report, NIST post-quantum standardization process
  Second round candidate of NIST post-quantum standardization process. LAC won the first prize in the Chinese post-quantum cryptography competition.

## Professional Activities

Program Committee of ProvSec 2020, ProvSec 2021.

Reviewer of ASIACRYPT 2015, 2018-21; PKC 2020-21; FC 2020; PQCrypto 2020; AsiaCCS 2019-21; ACISP 2017-21; Designs, Codes and Cryptography; Theoretical Computer Science, etc.

Invited Talks

- ✓ Efficient Online-friendly Two-Party ECDSA Signature
  Tsinghua University, Beijing, Nov. 2021
- ✓ Quantum-secure Authenticated Key Exchange from Supersingular Isogeny: New progress
  Shandong University, Qingdao, Nov. 2020;

- ✓ On the Constructions of Implicitly Authenticated Key Exchange
  East China Normal University, Shanghai, Oct. 2019
- ✓ Understanding and Constructing AKE via Double-key Key Encapsulation Mechanism
  ASIACRYPT 2018, Brisbane, Australia, Dec.2018

## Grants

| | |
|---|---|
| 2022-2025, PI, National Natural Science Foundation of China<br>On the Quantum-resistance of Authenticated Key Exchange | CNY 590,000 |
| 2020-2022, PI, Climbing Program of Chinese Academy of Sciences<br>Post-quantum Secure Authenticated Key Exchange | CNY 300,000 |
| 2019-2020, Co-PI, Science and Technology Major Project of Beijing<br>Quantum-resistant public key cryptosystems | CNY 2,500,000 |
| 2017-2019, PI, National Natural Science Foundation of China<br>Lossy Trapdoor Technique and Its Applications to Public Key Cryptography | CNY 220,000 |
| 2017-2019, PI, National Cryptography Development Fund<br>Basic Tools of Provable Security in Cryptography | CNY 100,000 |

## Awards

First Prize of Chinese post-quantum cryptography competition for LAC, 2020.

Second Prizes of Chinese post-quantum cryptography competition for SIAKE, 2020.

Best Paper Award of IWSEC 2015 (The 10th International Workshop on Security)

Best Paper Award of ProvSec 2014 (The 8th International Conference on Provable Security)

Outstanding Graduate of Shandong University in 2012

## Full Paper List

[1] Haiyang Xue, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui: Efficient Online-friendly Two-Party ECDSA Signature. **ACM CCS 2021**. pp. 558-573

[2] Haiyang Xue, Man Ho Au, Rupeng Yang, Bei Liang, Haodong Jiang: Compact Authenticated Key Exchange in the Quantum Random Oracle Model. **https://eprint.iacr.org/2020/1282**

[3] Haiyang Xue, Man Ho Au: Secure and Efficient Generic Two-Party Generation of Variants of ECDSA Signatures. **Manuscript**

[4] 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)

[5] Xiu Xu, Haiyang Xue, Kunpeng Wang, Man Ho Au, Song Tian: Strongly Secure Authenticated Key Exchange from Supersingular Isogenies. **ASIACRYPT (1) 2019**. pp. 278-308

[6] 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. **Secure Communication Networks** (2019)

[7] Zhengyu Zhang, Puwen Wei, Haiyang Xue: Tighter Security Proofs for Post-quantum Key Encapsulation Mechanism in the Multi-challenge Setting. **CANS 2019**. pp. 141-160

[8] Borui Gong, Man Ho Au, Haiyang Xue: Constructing Strong Designated Verifier Signatures from Key Encapsulation Mechanisms. **TrustCom/BigDataSE 2019**. pp. 586-593

[9] Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, Jingnan He: Understanding and Constructing AKE via Double-Key Key Encapsulation Mechanism. **ASIACRYPT (2) 2018**. pp. 158-189

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

[11] Yu Chen, Baodong Qin, Haiyang Xue: Regular lossy functions and their applications in leakage-resilient cryptography. **Theoretical Computer Science**. pp. 13-38 (2018)

[12] 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

[13] Daode Zhang, Kai Zhang, Bao Li, Xianhui Lu, Haiyang Xue, Jie Li: Lattice-Based Dual Receiver Encryption and More. **ACISP 2018**. pp. 520-538

[14] Daode Zhang, Bao Li, Yamin Liu, Haiyang Xue, Xianhui Lu, Dingding Jia: Towards Tightly Secure Deterministic Public Key Encryption. **ICICS 2017**. pp. 154-161

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

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

[17] 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**. pp. 34-49

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

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