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; Zero-knowledge proof.

Education

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

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

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

Working Experience

July 2015 - current	Assistant Professor, Institute of Information Engineering, Chinese Academy of Sciences
Sep. 2020 - current	Post-doctoral Research Fellow hosted by Associate Professor Man Ho Au Department of Computing, the Hong Kong Polytechnic University
Oct.2018 - Sep.2020	Post-doctoral Research Fellow hosted by Associate Professor Man Ho Au Department of Computer Sciences, the Hong Kong University

Highlights

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

Haiyang Xue

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

Selected Publications

- ✧ ***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 of Chinese post-quantum cryptography competition. This is the follow-up work of our theoretical paper in Asiacrypt 2019, by further proving the security of SIAKE 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, **ASIACRYPT 2019**.
  We propose two strongly secure authenticated key exchanges from supersingular isogenies in the random oracle model. It solves an open problem given by Galbraith.

- ✧ *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's post-quantum standardization process. A revisited version of LAC won the first prize of Chinese post-quantum cryptography competition.

- ✧ ***Haiyang Xue**, Xianhui Lu, Bao Li, Bei Liang, Jingnan He*
  Understanding and Constructing AKE via Double-key Key Encapsulation Mechanism, **ASIACRYPT 2018**.
  We find a common idea of constructing implicitly authenticated key exchange. Several famous works, such as HMQV, NAXOS, fit in our framework.

- ✧ *Yu Chen, Baodong Qin, **Haiyang Xue**:*
  Regularly Lossy Functions and Applications, **CT-RSA 2018**.
  We propose the primitive of regularly lossy function and investigate its applications in leakage-resilient (identity-based) key encapsulation mechanisms.

Professional Activities

Reviewer of ASIACRYPT 2015, 2018-20; FC 2020; ;PQCrypto 2020; AsiaCCS 2019-20; ACISP 2017-20; Designs, Codes and Cryptography; Theoretical Computer Science, etc.

Program Committee of the 14th International Conference on the theme of Provable and Practical Security (ProvSec 2020).

Invited Talks

- ✓ Quantum-secure Authenticated Key Exchange from Supersingular Isogeny--new progress
  Shandong University, Qingdao, Nov. 2020; Institute of Information Engineering, Beijing, Sep. 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 2020, Brisbane, Australia, Dec.2018; Hong Kong Polytechnic University, Jan. 2019

Haiyang Xue

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

Grants

PI, Climbing Program of Chinese Academy of Sciences, 2020-2022
Post-quantum Secure Authenticated Key Exchange

Co-PI, Science and Technology Major Project of Beijing Municipal Commission of Education, 2019-2020
Quantum-resistant public key cryptosystems

PI, National Natural Science Foundation of China, 2017-2019
Lossy Trapdoor Technique and Its Applications to Public Key Cryptography

PI, National Cryptography Development Fund, 2017-2019
Basic Tools of Provable Security in Cryptography

Awards

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

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

Best Paper Award IWSEC 2015

Best Paper Award ProvSec 2014

Outstanding 2012 Graduate of Shandong University

Full Publication List

[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 (1) 2019**: 278-308

[3] 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. **Secur. Commun. Networks** (2019)

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

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

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

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

[8] Yu Chen, Baodong Qin, Haiyang Xue: Regular lossy functions and their applications in leakage-resilient cryptography. **Theor. Comput. Sci.**: 13-38 (2018)

[9] 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

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

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

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

[13] 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)

[14] 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

[15] 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)

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