Haiyang Xue

haiyangxc@gmail.com | Personal Page | GoogleScholar | Github

Research Interests

- Theoretical cryptography and its applications. Focus on
    - Post-quantum cryptography
    - Authenticated key exchange
    - Zero knowledge proof

Education

IIE, Chinese Academy of Sciences Beijing
PhD of Cryptography in Information Security *Sep. 2012 – July 2015*

- "Lossy Trapdoor Related Primitives and Their Applications in Public Key Encryption."

Shandong University Jinan
Master in Information Security *Sep. 2009 – July 2012*
Bachelor in Mathematics *Sep. 2005 – July 2009*

Experience

Post-doctoral Fellow Feb. 2020 – Present
The University of Hong Kong *Hong Kong*

Post-doctoral Fellow Oct. 2018 – Feb. 2020
The Hong Kong Polytechnic University *Hong Kong*

Cryptography Researcher July 2015 – Sep. 2018
IIE, Chinese Academy of Sciences *Beijing*

Selected Publications

SIAKE: Supersingular Isogeny based Authenticated Key Exchange *CACR-PQC*

- Haiyang Xue, Xianhui Lu, Kunpeng Wang, Song Tian, Xiu Xu, Jingnan He, Bao Li
- Second prize of Chinese post-quantum cryptography competition

Strongly Secure Authenticated Key Exchange from Supersingular Isogenies *ASIACRYPT 2019*

- Xiu Xu, Haiyang Xue, Kunpeng Wang, Man Ho Au, Song Tian

LAC: Lattice-based Cryptosystem *NIST-PQC*

- Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, Kunpeng Wang
- 2nd round, NIST post-quantum cryptography standardization process.
- First prize of Chinese post-quantum cryptography competition

Understanding and Constructing AKE via Double-key Key Encapsulation Mechanism *ASIACRYPT 2018*

- Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, Jingnan He

Regularly Lossy Functions and Applications *CT-RSA 2018*

- Yu Chen, Baodong Qin, Haiyang Xue

Regular lossy functions and their applications in leakage-resilient cryptography *TCS 2018*

- Yu Chen, Baodong Qin, Haiyang Xue

Research Funding

PI, Climbing Program 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

Academic Service

Reviewer of ASIACRYPT 2015, 2018-2020; FC 2020; PQCrypto 2020; ACISP 2017-2020 etc.

PC member of ProvSec 2020

Awards

First Prize (LAC.PKE) of Chinese post-quantum cryptography competition.

Second Prizes (SIAKE, LAC.KEX) of Chinese post-quantum cryptography competition.

Best Paper Award IWSEC 2015

Best Paper Award ProvSec 2014

Please refer the next page for my full publications.

Full 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 (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

Before 2017

[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

[14] 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

[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

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