Curriculum Vitae

PQ810, Department of Computing,
The Hong Kong Polytechnic University, Hong Kong
Phone: +85257631077
Email: haiyangxc@gmail.com
Homepage: https://haiyangxc.github.io/hyxue/

Research Interests

I am broadly interested in cryptography and its applications in cybersecurity, including but not limited to,

Post-quantum cryptography, especially authenticated key exchange from lattice and isogenies,
Multiparty computation, especially threshold cryptography,
Zero-knowledge proof, etc.

Education

PhD, Institute of Information Engineering, Chinese Academy of Sciences, 2015
Thesis: Public Key Cryptosystems from Lossy Trapdoor Primitives, Supervisor: Bao Li

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

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

Working Experience

Dec.2022 - current	Research Assistant Professor, Department of Computing, PolyU
Jan.2022 - Nov.2022	Research Assistant Professor, Department of Computer Science, HKU
Jul.2015 - Nov.2021	Researcher, Institute of Information Engineering, Chinese Academy of Sciences
Sep.2020 - Sep.2021	Visiting Scholar, Department of Computer Science, HKU
Oct.2018 - Sep. 2020	Visiting Scholar, Department of Computing, PolyU

Grants

On the Quantum-resistance of Authenticated Key Exchange, 2022-2025, National Natural Science Foundation of China, RMB 590,000, Principal Investigator

Post-quantum Secure Authenticated Key Exchange, 2020-2022, Climbing Program of Chinese Academy of Sciences, RMB 300,000, Principal Investigator

Quantum-resistant Public Key Cryptosystems, 2019-2020, Science and Technology Major Project of Beijing, RMB 2,500,000, Co-Investigator

Lossy Trapdoor Technique and Its Applications to Public Key Cryptography, 2017-2019, National Natural Science Foundation of China, RMB 220,000, Principal Investigator

Basic Tools of Provable Security, 2017-2019, National Cryptography Development Fund, RMB 100,000, Principal Investigator

Awards

- ✓ Merit Prize in the "Fintech-Cryptography" competition organized by the People's Bank of China and Tsinghua University, 2022
- ✓ First Prize in the Chinese post-quantum cryptography competition for LAC.PKE, held by the Chinese Association for Cryptologic Research (CACR), 2020.
- ✓ Two Second Prizes in the Chinese post-quantum cryptography competition for SIAKE, LAC.KEX, held by CACR, 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)

Teaching

COMP6712[1] Advanced Security and Privacy, 2022/23 Semester 2

Selected Publications

2 A* and 2 A conference papers according to CORE Ranking

- ✧ ***Haiyang Xue****, Man Ho Au, Mengling Liu, Kwan Yin Chan, Handong Cui, Xiang Xie, Tsz Hon Yuen, Chengru Zhang:* Efficient Multiplicative-to-Additive Function from Joye-Libert Cryptosystem and Its Application to Threshold ECDSA. The 30th ACM Conference on Computer and Communications Security (ACM CCS 2023)
  We propose a multiplicative-to-additive (MtA) function from the Joye-Libert scheme which outperforms the state-of-the-art function from Paillier. Our approach has the best trade-off between computation and communication. As an important building block, our MtA function can be used to design efficient threshold ECDSA, which could further secure cryptocurrency wallet.

- ✧ ***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), pages 558-573 (2021) Acceptance Rate: 22.2%
  We propose an online-friendly two-party ECDSA with a lightweight online phase and a single multiplicative-to-additive function in the offline phase. While maintaining extremely fast online computation, our solution has the best overall performance.

- ✧ *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. Our solution benefits the compact structure and achieves the strongest AKE security. It solves

[1] The course website: https://haiyangxc.github.io/hyxue/teaching/comp6712-23.html

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 enhancing the understanding of how to construct authenticated key exchange which is known to be complicated and error-prone, and captures celebrated works including HMQC, and 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
A lattice-based cryptosystem using smallest modulus (Byte-Level modulus). Second-round candidate in the NIST post-quantum standardization process and received the first prize in the Chinese post-quantum cryptography competition.

Professional Activities

Program Committee of Inscrypt 2023, IPSEC 2023, ProvSec 2023, ProvSec 2022, ProvSec 2021, ProvSec 2020.

Reviewer of ASIACRYPT 2015, 2018-22; PKC 2020-21; FC 2020; PQCrypto 2020; AsiaCCS 2019-21; ACISP 2017-22; Designs, Codes and Cryptography; Theoretical Computer Science, etc.

Selected Talks

✓ Securing Your Wallet with Threshold Cryptography
HKU-SCF Fintech Talk, Hong Kong, Sep. 2022

✓ Efficient Online-friendly Two-Party ECDSA Signature
Tsinghua University, Beijing, Nov. 2021; Shandong University, Jinan, Jun. 2022

✓ Quantum-secure Authenticated Key Exchange from Supersingular Isogeny: New progress
Shandong University, Qingdao, Nov. 2020;

✓ On the Construction of Implicitly Authenticated Key Exchange
East China Normal University, Shanghai, Oct. 2019

Patents

Granted: Man Ho Au, Haiyang Xue, Rupeng Yang, Borui Gong, and Wang Fat Lau, 保护数据隐私的多方联合处理数据的方法及装置, China Patent CN111885079A, 2017

Granted: Jia Fan, Wei Zhao, Yunfei Cao, Haiyang Xue, Bao Li, and Xianhui Lu, 一种基于位置和口令的密钥交换协议, China Patent CN108270572A, 2020

Full Paper List

3 A*, 3 A, and 7 B papers according to CORE Ranking

[1] Haiyang Xue, Man Ho Au, Mengling Liu, Kwan Yin Chan, Handong Cui Xiang Xie, Tsz Hon Yuen, Chengru Zhang: Efficient Multiplicative-to-Additive Function from Joye-Libert Cryptosystem and Its Application to Threshold ECDSA. **ACM CCS 2023**. pp. ???-???

[2] Chengliang Tian, Jia Yu, Hanlin Zhang, Haiyang Xue, Cong Wang, Kui Ren: Novel Secure Outsourcing of Modular Inversion for Arbitrary and Variable Modulus. **IEEE Transactions on Services Computing** 2022. pp. 241-253

[3] Handong Zhang, Puwen Wei, Haiyang Xue, Yi Deng, Jinsong Li, Wei Wang, Guoxiao Liu: Resumable ZeroKnowledge for Circuits from Symmetric Key Primitives. **ACISP 2022**. pp. 375–398

[4] 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

[5] Haiyang Xue, Xianhui Lu, Kunpeng Wang, Song Tian, Xiu Xu, Jingnan He, Bao Li: SIAKE: Supersingular Isogeny based Authenticated Key Exchange, **Second prize in the Chinese post-quantum competition**

[6] 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**

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

[8] Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, Kunpeng Wang LAC: Lattice-based Cryptosystem, **NIST post-quantum standardization process**

[9] 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

[10] 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)

[11] 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

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

[13] 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

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

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

[16] 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

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

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

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

[20] 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 Award**)

[21] 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

[22] 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 Award**)

[23] Mingqiang Wang, Haiyang Xue, Tao Zhan: Fault attacks on hyperelliptic curve discrete logarithm problem over binary field. **Sci. China Inf. Sci**. 57(3): 1-17 (2014)

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