

目前为香港大学计算机学院研究助理教授(研究),对理论密码学与应用密码学的研究感兴趣,希望对理论密码学及其应用的推进做出贡献。

## 研究兴趣

- ✓ 理论与应用密码学
- ✓ 后量子密码学, 尤其基于格和同源的认证密钥交换
- ✓ 多方安全计算, 零知识证明等

## 教育背景

- ✓ 2012.09-2015.07 工学博士(信息安全), 中科院信息工程研究所, 信安国重, 导师: 李宝
- ✓ 2009.09-2012.07 硕士(密码学), 山东大学, 数学学院, 导师: 王明强
- ✓ 2005.09-2009.07 学士(信息安全), 山东大学, 数学学院

## 工作经历

- ✓ 2022.01-至今 助理教授(研究), 香港大学, 计算机学院
- ✓ 2015.09-2021.12 助理研究员, 中国科学院信息工程研究所, 信息安全国家重点实验室
- ✓ 2020.10-2021.08 博士后, 香港大学, 计算机学院
- ✓ 2018.09-2020.10 博士后, 香港理工大学, 计算机学院

## 主要贡献

- ✓ 项目: 主持国家自然科学基金面上一项, 青年一项; 主持十三五密码发展基金等项目
- ✓ 密码算法设计: 基于格设计的 LAC 算法为亚洲唯一进入 NIST 后量子标准化第二轮的算法, 获全国密码算法设计一等奖;  
基于同源设计的 SIAKE 密码算法获全国密码算法设计二等奖
- ✓ 论文: 发表密码国际顶级会议 ACM CCS 2021, ASIACRYPT 2018-2019 等 19+篇

## 科研项目

- ✓ 2022-2025 国家自然科学基金面上 62172412 “抗量子安全认证密钥交换的关键技术研究”
- ✓ 2017-2019 国家自然科学基金青年 61602473 “损耗陷门技术及其在公钥密码中的应用”
- ✓ 2017-2019 十三五密码发展基金 “可证明安全基础工具的研究”
- ✓ 2019-2020 北京市科委项目 “抗量子密码算法设计理论与技术研究”(骨干)
- ✓ 2020-2022 中国科学院所级攀登计划 “后量子安全认证密钥交换”

## 获奖情况

- ✓ LAC 算法: 全国密码算法设计一等奖(2020)
- ✓ SIAKE 算法: 全国密码算法设计二等奖(2020)
- ✓ ProvSec 2014 与 IWSEC 2015 最佳论文
- ✓ 2012 年山东省优秀硕士毕业生

代表工作

- ✓ **Haiyang Xue, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui: Efficient Online-friendly Two-Party ECDSA Signature, CCS 2021.**  
我们设计了一个在线友好的高效的两方 ECDSA 签名算法,其离线的计算只需要依赖单个的 MTA 函数。成果发表在安全顶会 CCS 2021
- ✓ **Haiyang Xue, Xianhui Lu, Kunpeng Wang, Song Tian, Xiu Xu, Jingnan He, Bao Li: SIAKE: Supersingular Isogeny based Authenticated Key Exchange, Technical Report, 全国密码算法设计**  
我们在 ASIACRYPT2019 基础上设计基于同源的后量子安全认证密钥交换; 获得全国密码算法设计二等奖
- ✓ **Xiu Xu, Haiyang Xue\*, Kunpeng Wang, Man Ho Au, Song Tian: Strongly Secure Authenticated Key Exchange from Supersingular Isogenies, ASIACRYPT 2019.**  
我们基于同源问题给出了一个高安全的认证密钥交换, 解决了著名密码学家 Steven Galbraith 提出的公开问题, 成果发表在密码顶会亚密 2019
- ✓ **Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, Jingnan He: Understanding and Constructing AKE via Double-key Key Encapsulation Mechanism, ASIACRYPT 2018.**  
我们给出了认证密钥交换的统一框架, 不仅解释了注明的 HMQV, NAXOS, 而且引出后量子安全认证密钥交换, 成果发表在密码顶会亚密 2018
- ✓ **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**  
我们基于格问题设计了后量子安全的 LAC 算法, 为亚洲唯一进入 NIST 后量子标准化的第二轮的算法, 获得全国密码算法设计一等奖

学术工作

- ✓ 会议委员会: ProvSec 2020 和 ProvSec 2021
- ✓ 审稿人: ASIACRYPT 2015, 2018-21; FC 2020; PQCrypto 2020; AsiaCCS 2019-21; ACISP 2017-21; Designs, Codes and Cryptography; Theoretical Computer Science 等
- ✓ 部分报告:
  - ✧ 基于同源的后量子认证密钥交换  
中国密码学会密码算法设计高端培训, 2021 年 8 月
  - ✧ Quantum-secure Authenticated Key Exchange from Supersingular Isogeny: New progress  
山东大学, 2020 年 12 月; 中科院信工所 (在线), 2021 年 3 月
  - ✧ On the Constructions of Implicitly Authenticated Key Exchange  
华东师范大学, 2020 年 10 月
  - ✧ Strongly Secure Authenticated Key Exchange from Supersingular Isogenies  
亚密, 日本, 2019 年 12 月
  - ✧ Understanding and Constructing AKE via Double-key Key Encapsulation Mechanism  
亚密, 澳大利亚, 2018 年 12 月

完整论文列表

- [1] Haiyang Xue, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui: Efficient Online-friendly Two-Party ECDSA Signature. **ACM CCS 2021**: 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**: 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**: 141-160
- [8] Borui Gong, Man Ho Au, Haiyang Xue: Constructing Strong Designated Verifier Signatures from Key Encapsulation Mechanisms. **TrustCom/BigDataSE 2019**: 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**: 158-189
- [10] Yu Chen, Baodong Qin, **Haiyang Xue**: Regularly Lossy Functions and Applications. **CT-RSA 2018**: 491-511
- [11] Yu Chen, Baodong Qin, **Haiyang Xue**: Regular lossy functions and their applications in leakage-resilient cryptography. **Theoretical Computer Science**: 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**: 520-538
- [14] Daode Zhang, Bao Li, Yamin Liu, **Haiyang Xue**, Xianhui Lu, Dingding Jia: Towards Tightly Secure Deterministic Public Key Encryption. **ICICS 2017**: 154-161
- [15] **Haiyang Xue**, Yamin Liu, Xianhui Lu, Bao Li: Lossy Projective Hashing and Its Applications. **INDOCRYPT 2015**: 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**: 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**: 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**: 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**: 235-250