Zhedong Wang

CURRENT POSITION

Florida Atlantic University   *Jul 2019 - Current*

Postdoctoral Fellow in Cryptography

Supported by NSF CRII Award (CNS-1657040) and NSF Career Award (CNS-1942400)

College of Engineering and Computer Science

Phone: +1 4016628957

Email: wangz@fau.edu

Supervisor: Prof. Feng-Hao Liu

Personal Website: https://wangz2019.github.io

RESEARCH INTERESTS

- My main interests are in cryptography; especially

    - Post-quantum Cryptography

    - Lattice-based Cryptography: Fully Homomorphic Encryption, Identity-based Encryption, Attribute-based Encryption, Functional Encryption

    - Leakage and Tampering Resilient Cryptography

- I am also interested in computational complexity and algebraic number theory

EDUCATION

University of Chinese Academy of Sciences   *Sep 2013 - Jun 2019*

Ph.D. in Cryptography & Information Security

State Key Laboratory of Information Security (SKLOIS)

Advisors: Prof. Mingsheng Wang and Prof. Feng-Hao Liu (co-advised at FAU)

Thesis: Research on Lattice-based Public Key Cryptosystems Design and Tight Security

Sichuan University   *Sep 2009 - Jun 2013*

B.S. in Mathematics

TEACHING EXPERIENCES

- Guest Lecturer for COT 6930: Cryptography under Physical Attacks   Fall 2019

    - Presented Entropy and Randomness Extraction

    - Instructor: Feng-Hao Liu

    - Florida Atlantic University, FL

- Guest Lecturer for COT 6200: Computational Complexity   Fall 2017

    - Hosted student presentations

    - Instructor: Feng-Hao Liu

    - Florida Atlantic University, FL

- Teaching Assistant for 201M4001H: The Mathematical Foundations of Cryptography   Fall 2016

    - Graded assignments and exams

– Instructor: Mingsheng Wang and Yongqiang Li

– University of Chinese Academy of Sciences, Beijing.

VISITING EXPERIENCES

- Simons Institute for the Theory of Computing, UC Berkeley, CA   Feb 2020

    – Event: Workshop

    – Topic: Lattices: Geometry, Algorithms and Hardness

- Florida Atlantic University, Boca Raton, FL   Sep 2017 - Nov 2018

    – Mentor: Feng-Hao Liu

    – Topic: Design and analysis on new randomized algorithm

PUBLICATIONS

Publications in Print

- **Conference Publications**

    1 Feng-Hao Liu, <u>Zhedong Wang</u>. **Rounding in the Rings**. In Annual International Cryptology Conference (CRYPTO), 2020.

    2 Qiqi Lai, Feng-Hao Liu, <u>Zhedong Wang</u>. **Almost Tight Security in Lattices with Polynomial Moduli - PRF, IBE, All-but-many LTF, and More**. In Proceedings of the 23th International Conference on Practice and Theory of Public Key Cryptography (PKC), 2020.

    3 <u>Zhedong Wang</u>, Xiong Fan, Feng-Hao Liu. **FE for Inner Products and Its Application to Decentralized ABE**. In Proceedings of the 22th International Conference on Practice and Theory of Public Key Cryptography (PKC), 2019.

    4 <u>Zhedong Wang</u>, Xiong Fan and Mingsheng Wang. **Compact Inner Product Encryption from LWE**. In Proceedings of the 19th International Conference on Information and Communications Security (ICICS), 2017.

- **Journal Publications**

    1 Yuan Chen, Qingkuan Dong, Yannan Li, Qiqi Lai and <u>Zhedong Wang</u>. **Natural sd-RCCA Secure Public-key Encryptions from Hybrid Paradigms**. Journal of Universal Computer Science, vol. 25, no. 3 (2019), 158-181.

Manuscripts

1 Qiqi Lai, Feng-Hao Liu, Zhedong Wang. **Rate-1 Key-Dependent Message Security via Reusable Homomorphic Extractor against Correlated-Source Attacks**. 2020.

2 Qiqi Lai, Feng-Hao Liu, Zhedong Wang. **Leakage-resilient ABE with Optimal Leakage Rates from Lattices**. 2020.

3 Mingsheng Wang, Xi Lin, Heyang Cao, Feng-Hao Liu, Zhedong Wang. **Prcatical (ℓ-more) Extractable Hash Functions from Ideal Lattices**. 2020.

SCIENTIFIC PRESENTATIONS

- Algebraically Structured Learning with Rounding (LWR)

- – Florida Atlantic University, FL, US   Aug 2020
- Almost Tight Security in Lattices
  - – Florida Atlantic University, FL, US   Feb 2020
- FE for Inner Products and Its Application to Decentralized ABE
  - – PKC 2019, Beijing China   Apr 2019

AWARDS

- Travel Grant, Simons Institute for the Theory of Computing, CA   2020
- National Scholarship for Encouragement, China,   Dec 2012

PROFESSIONAL SERVICES

- External Reviewer: PKC 2021, CRYPTO 2020, Asiacrypt 2020, PKC 2019, Asiacrypt 2019, IEEE Access.