Feng-Hao Liu

Institutional Affication

School of EECS
Washington State University (WSU)

Contact

Email: feng-hao.liu@wsu.edu
Address: EME 402,
355 NE Spokane St. PO Box 642752
Pullman, WA, 99164-2752 U.S.A.
Webpage: https://fenghaoliu.github.io

Research Areas

- Lattice-based cryptography
- Fully Homomorphic Encryption, theory and applications to private data analytics, machine learning
- Post-quantum cryptography for advanced crypto designs, including functional encryption, attribute-based encryption, advanced signatures, efficient lattice zero-knowledge proofs
- Leakage and tamper resilient cryptography
- Multiparty computation

Education

Ph.D. Computer Science — Sep 2009 - May 2013
Brown University, Providence, RI.
Thesis: "*Error Tolerant Cryptography*"
Advisor: Anna Lysyanskaya

Sc.M. Computer Science — Sep 2007 - May 2009
Brown University, Providence, RI.

B.S. Electrical Engineering — Sep 2001- Jun 2005
National Taiwan University, Taipei, Taiwan.
Minor: Mathematics

Employment History

Associate Professor, Washington State University, Pullman, WA. Aug 2023 - present
Visiting Associate Professor, Florida Atlantic University, Boca Raton, FL. Aug 2023 - present
Associate Professor, Florida Atlantic University, Boca Raton, FL. Aug 2021 - July 2023
Assistant Professor, Florida Atlantic University, Boca Raton, FL. May 2015 - July 2021

- Awarded prestigious external funds, such as **NSF CRII Award** and **NSF Career Award**
- Awarded FAU Junior Faculty Research Award 2021
- Mentoring postdoc, graduate and undergraduate students, and visiting scholars
- Developing international partnerships to host exchange graduate students
- Developed new graduate courses *COT 6930: Cryptography under Physical Attacks*, *COT 6930: Computation on Encrypted Data* to achieve broader impacts
- Developed a new undergraduate course *COT 4930: Competitive Programming*
- Gave invited talks, ranging from research talks at conferences/universities to introductory lectures at high schools for broader impacts
- Served as professional reviewers for major IACR cryptography conferences and an NSF panel

Consultant, Inventec, Taipei, Taiwan Jan 2022 - present

- Researching and developing practical cryptographic solutions to enhance privacy of machine learning, such as
  - Using FHE to protect privacy of neural network models/inferences, with efficient homomorphic algorithm/architecture designs
  - Identifying new FHE-friendly machine learning models to accelerate homomorphic computation
  - Deploying Zero-knowledge proofs efficiently to achieve practical image assurance

Consultant, BTQ, Taipei, Taiwan Jan 2023 - present

- Researching and developing practical post quantum cryptographic schemes, such as
  - Post-quantum zero-knowledge proofs, polynomial commitments, signatures, etc.

Postdoc Researcher, Maryland Cybersecurity Center @UMD, College Park, MD. July 2013 - May 2015

- Hosted by Prof. Jonathan Katz, Prof. Elaine Shi and Prof. Dana Dachman-Soled

Research Assistant, Dept. of Computer Science, Brown U., Providence, RI. Sep 2009 - May 2013

- Advised by Prof. Anna Lysyanskaya

Summer Intern, Microsoft Research, Redmond, WA. Jun 2012 - Aug 2012

- Mentored by Dr. Melissa Chase and Dr. Nishanth Chandran in the Crypto Group
- Investigated different applications of re-encryption, relaxations of obfuscation, and lattice-based constructions

Research Assistant, IIS, Academia Sinica, Taipei, Taiwan. Dec 2006 - Jun 2007

- Advised by Prof. Bo-Yin Yang
- Implemented several multivariate cryptographic systems, in Java and C++
- Investigated a new stream cipher QUAD, and made generalizations and improvements

Second Lieutenant, Chung Cheng Armed Forces Prep School, Kaohsiung, Taiwan. Jul 2005 - Oct 2006

- Oversaw over 80 senior high school students, teaching both discipline and academic studies
- Advised as a math teaching assistant that increased average math scores and admission rates of all senior students by 15%, from 75% to 90%

Publications

- The authorships in crypto related venues (e.g., the IACR conferences including Crypto, Eurocrypt, Asiacrypt, TCC, PKC, Journal of Cryptology) are mostly listed alphabetically by the last names.
- All the papers are peer-reviewed.

Conference and Journal Papers

39. Efficient Multiparty Probabilistic Threshold Private Set Intersection, with En Zhang and Leiyong Qin. In CCS 2023

38. An Efficient CKKS-FHEW/TFHE Hybrid Encrypted Inference Framework, with Tzu-Li Liu, Yu-Te Ku, Ming-Chien Ho, Ming-Ching Chang, Chih-Fan Hsu, Wei-Chao Chen and Shih-Hao Hung. In PriST-AI 2023, a workshop of ESORICS 2023

37. Region-aware Photo Assurance System for Image Authentication, with Ke-Han Li, Chih-Fan Hsu, Ming-Ching Chang, Shao-Yi Chien and Wei-Chao Chen. In MIPR 2023

36. Feng-Hao Liu and Han Wang. Batch bootstrapping II: Bootstrapping in polynomial modulus only requires $\tilde{O}(1)$ FHE multiplications in amortization. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part III*, volume 14006 of *Lecture Notes in Computer Science*, pages 353–384, Lyon, France, April 23–27, 2023. Springer, Heidelberg, Germany

35. Feng-Hao Liu and Han Wang. Batch bootstrapping I: A new framework for SIMD bootstrapping in polynomial modulus. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part III*, volume 14006 of *Lecture Notes in Computer Science*, pages 321–352, Lyon, France, April 23–27, 2023. Springer, Heidelberg, Germany

34. Daniel Apon, Chloé Cachet, Benjamin Fuller, Peter Hall, and Feng-Hao Liu. Nonmalleable digital lockers and robust fuzzy extractors in the plain model. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022, Part IV*, volume 13794 of *Lecture Notes in Computer Science*, pages 353–383, Taipei, Taiwan, December 5–9, 2022. Springer, Heidelberg, Germany

33. Chih-Fan Hsu, Jing-Lun Huang, Feng-Hao Liu, Ming-Ching Chang, and Wei-Chao Chen. Fedtrust: Towards building secure robust and trustworthy moderators for federated learning. In *5th IEEE International Conference on Multimedia Information Processing and Retrieval, MIPR 2022, Virtual Event, USA, August 2-4, 2022*, pages 318–323. IEEE, 2022

32. Qiqi Lai, Feng-Hao Liu, and Zhedong Wang. Leakage-resilient IBE/ ABE with optimal leakage rates from lattices. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022: 25th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 13178 of *Lecture Notes in Computer Science*, pages 225–255, Virtual Event, March 8–11, 2022. Springer, Heidelberg, Germany

31. Parhat Abla, Feng-Hao Liu, Han Wang, and Zhedong Wang. Ring-based identity based encryption - asymptotically shorter MPK and tighter security. In Kobbi Nissim and Brent Waters, editors, *TCC 2021: 19th Theory of Cryptography Conference, Part III*, volume 13044 of *Lecture Notes in Computer Science*, pages 157–187, Raleigh, NC, USA, November 8–11, 2021. Springer, Heidelberg, Germany

30. Qiqi Lai, Feng-Hao Liu, and Zhedong Wang. New lattice two-stage sampling technique and its applications to functional encryption - stronger security and smaller ciphertexts. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 498–527, Zagreb, Croatia, October 17–21, 2021. Springer, Heidelberg, Germany

29. Qiqi Lai, Feng-Hao Liu, and Zhedong Wang. Rate-1 key-dependent message security via reusable homomorphic extractor against correlated-source attacks. In Juan Garay, editor, *PKC 2021: 24th International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 12710 of *Lecture Notes in Computer Science*, pages 421–450, Virtual Event, May 10–13, 2021. Springer, Heidelberg, Germany

28. Feng-Hao Liu and Zhedong Wang. Rounding in the rings. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020, Part II*, volume 12171 of *Lecture Notes in Computer Science*, pages 296–326, Santa Barbara, CA, USA, August 17–21, 2020. Springer, Heidelberg, Germany

27. Dana Dachman-Soled, Feng-Hao Liu, Elaine Shi, and Hong-Sheng Zhou. Locally decodable and updatable non-malleable codes and their applications. *Journal of Cryptology*, 33(1):319–355, January 2020

26. Qiqi Lai, Feng-Hao Liu, and Zhedong Wang. Almost tight security in lattices with polynomial moduli - PRF, IBE, all-but-many LTF, and more. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020: 23rd International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 12110 of *Lecture Notes in Computer Science*, pages 652–681, Edinburgh, UK, May 4–7, 2020. Springer, Heidelberg, Germany

25. En Zhang, Feng-Hao Liu, Qiqi Lai, Ganggang Jin, and Yu Li. Efficient multi-party private set intersection against malicious adversaries. In Radu Sion and Charalampos Papamanthou, editors, *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop, CCSW@CCS 2019, London, UK, November 11, 2019*, pages 93–104. ACM, 2019

24. Dana Dachman-Soled, S. Dov Gordon, Feng-Hao Liu, Adam O'Neill, and Hong-Sheng Zhou. Leakage resilience from program obfuscation. *Journal of Cryptology*, 32(3):742–824, July 2019

23. Xiong Fan and Feng-Hao Liu. Proxy re-encryption and re-signatures from lattices. In Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung, editors, *ACNS 19: 17th International Conference on Applied Cryptography and Network Security*, volume 11464 of *Lecture Notes in Computer Science*, pages 363–382, Bogota, Colombia, June 5–7, 2019. Springer, Heidelberg, Germany

22. Zhedong Wang, Xiong Fan, and Feng-Hao Liu. FE for inner products and its application to decentralized ABE. In Dongdai Lin and Kazue Sako, editors, *PKC 2019: 22nd International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 11443 of *Lecture Notes in Computer Science*, pages 97–127, Beijing, China, April 14–17, 2019. Springer, Heidelberg, Germany

21. David Cash, Feng-Hao Liu, Adam O'Neill, Mark Zhandry, and Cong Zhang. Parameter-hiding order revealing encryption. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 181–210, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Heidelberg, Germany

20. Aggelos Kiayias, Feng-Hao Liu, and Yiannis Tselekounis. Non-malleable codes for partial functions with manipulation detection. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 577–607, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany

19. Daniel Apon, Xiong Fan, and Feng-Hao Liu. Deniable attribute based encryption for branching programs from LWE. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B: 14th Theory of Cryptography Conference, Part II*, volume 9986 of *Lecture Notes in Computer Science*, pages 299–329, Beijing, China, October 31 – November 3, 2016. Springer, Heidelberg, Germany

18. Aggelos Kiayias, Feng-Hao Liu, and Yiannis Tselekounis. Practical non-malleable codes from l-more extractable hash functions. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 2016: 23rd Conference on Computer and Communications Security*, pages 1317–1328, Vienna, Austria, October 24–28, 2016. ACM Press

17. Dana Dachman-Soled, S. Dov Gordon, Feng-Hao Liu, Adam O'Neill, and Hong-Sheng Zhou. Leakage-resilient public-key encryption from obfuscation. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *PKC 2016: 19th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 9615 of *Lecture Notes in Computer Science*, pages 101–128, Taipei, Taiwan, March 6–9, 2016. Springer, Heidelberg, Germany

16. S. Dov Gordon, Feng-Hao Liu, and Elaine Shi. Constant-round MPC with fairness and guarantee of output delivery. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 63–82, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany

15. Dana Dachman-Soled, Feng-Hao Liu, and Hong-Sheng Zhou. Leakage-resilient circuits revisited - optimal number of computing components without leak-free hardware. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 131–158, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany

14. S. Dov Gordon, Jonathan Katz, Feng-Hao Liu, Elaine Shi, and Hong-Sheng Zhou. Multi-client verifiable computation with stronger security guarantees. In Yevgeniy Dodis and Jesper Buus Nielsen,

editors, *TCC 2015: 12th Theory of Cryptography Conference, Part II*, volume 9015 of *Lecture Notes in Computer Science*, pages 144–168, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany

13. Dana Dachman-Soled, Feng-Hao Liu, Elaine Shi, and Hong-Sheng Zhou. Locally decodable and updatable non-malleable codes and their applications. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015: 12th Theory of Cryptography Conference, Part I*, volume 9014 of *Lecture Notes in Computer Science*, pages 427–450, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany

12. Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou. Multi-input functional encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 578–602, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany

11. Nishanth Chandran, Melissa Chase, Feng-Hao Liu, Ryo Nishimaki, and Keita Xagawa. Re-encryption, functional re-encryption, and multi-hop re-encryption: A framework for achieving obfuscation-based security and instantiations from lattices. In Hugo Krawczyk, editor, *PKC 2014: 17th International Conference on Theory and Practice of Public Key Cryptography*, volume 8383 of *Lecture Notes in Computer Science*, pages 95–112, Buenos Aires, Argentina, March 26–28, 2014. Springer, Heidelberg, Germany

10. Alexandra Berkoff and Feng-Hao Liu. Leakage resilient fully homomorphic encryption. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 515–539, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany

9. Kai-Min Chung, Daniel Dadush, Feng-Hao Liu, and Chris Peikert. On the lattice smoothing parameter problem. In *Proceedings of the 28th Conference on Computational Complexity, CCC 2013, Palo Alto, California, USA, 5-7 June, 2013*, pages 230–241. IEEE Computer Society, 2013

8. Feng-Hao Liu and Anna Lysyanskaya. Tamper and leakage resilience in the split-state model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 517–532, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Heidelberg, Germany

7. Yun-Ju Huang, Feng-Hao Liu, and Bo-Yin Yang. Public-key cryptography from new multivariate quadratic assumptions. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 190–205, Darmstadt, Germany, May 21–23, 2012. Springer, Heidelberg, Germany

6. Kai-Min Chung, Yael Tauman Kalai, Feng-Hao Liu, and Ran Raz. Memory delegation. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 151–168, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany

5. Ching-Hua Yu, Sherman S. M. Chow, Kai-Min Chung, and Feng-Hao Liu. Efficient secure two-party exponentiation. In Aggelos Kiayias, editor, *Topics in Cryptology – CT-RSA 2011*, volume 6558 of *Lecture Notes in Computer Science*, pages 17–32, San Francisco, CA, USA, February 14–18, 2011. Springer, Heidelberg, Germany

4. Kai-Min Chung, Feng-Hao Liu, Chi-Jen Lu, and Bo-Yin Yang. Efficient string-commitment from weak bit-commitment. In Masayuki Abe, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 268–282, Singapore, December 5–9, 2010. Springer, Heidelberg, Germany

3. Feng-Hao Liu and Anna Lysyanskaya. Algorithmic tamper-proof security under probing attacks. In Juan A. Garay and Roberto De Prisco, editors, *SCN 10: 7th International Conference on Security in Communication Networks*, volume 6280 of *Lecture Notes in Computer Science*, pages 106–120, Amalfi, Italy, September 13–15, 2010. Springer, Heidelberg, Germany

2. Kai-Min Chung and Feng-Hao Liu. Parallel repetition theorems for interactive arguments. In Daniele Micciancio, editor, *TCC 2010: 7th Theory of Cryptography Conference*, volume 5978 of *Lecture Notes in Computer Science*, pages 19–36, Zurich, Switzerland, February 9–11, 2010. Springer, Heidelberg, Germany

1. Feng-Hao Liu, Chi-Jen Lu, and Bo-Yin Yang. Secure PRNGs from specialized polynomial maps over any. In Johannes Buchmann and Jintai Ding, editors, *Post-quantum cryptography, second international workshop, PQCRYPTO 2008*, pages 181–202, Cincinnati, Ohio, United States, October 17–19, 2008. Springer, Heidelberg, Germany

Book Chapter

1. *"Computation Over Encrypted Data."* Invited Book Chapter of *"Cloud Computing Security: Foundations and Challenges"*, Editor, John Vacca, CRC Press, ISBN 978-1482260946. 2016.

Invited Research Lectures

Efficient Multiparty Probabilistic Threshold Private Set Intersection

- CCS, Copenhagen, Denmark Nov 2023

Cryptography in the Presence of Quantum Computing: New Opportunities and Research Directions

- Washington State University Nov 2023
  Cyser Seminar

Post-quantum Cryptography and Fully Homomorphic Encryption

- National Taiwan University Sep 2022

Ring-based Identity-based Encryption

- Shanghai Jiaotong University, China Mar 2022

- Shaanxi Normal University, China Jan 2022

Crypto and I

- FAU High School Oct 2021
  Invited speaker at the course Introduction to Research

Rounding in the Rings

- ENS de Lyon, Royal Holloway, and CWI Feb 2021
  Joint Crypto Seminar

Next Generation of Information Security

- Florida Atlantic University, FL Nov 2020
  Research in Action

Efficient Multi-Party Private Set Intersection Against Malicious Adversaries

- Chinese Academy of Sciences, China Dec 2019
- Shaanxi Normal University, China Dec 2019
- Henan Normal University, China Dec 2019
- CCSW@London, UK Nov 2019

Tight Reduction in Lattices.

- Chinese Academy of Sciences, China May 2019
- Shaanxi Normal University, China May 2019

First Byte of Cyber Security and Cryptography .

- FAU High School, USA Nov 2018
  NIST National Cybersecurity Career Awareness Week

Improved Identity-based Encryption from Lattices.

- Chongqing University, China Dec 2017
- Tsinghua University, China Dec 2016

Constant-Round MPC with Fairness and Guarantee of Output Delivery.

- Florida Atlantic University (CCIS Seminar), USA Sep 2015
- Crypto, Santa Barbara, USA Aug 2015

Computation in the Presence of Leakage.

- United States Naval Academy, USA Dec 2014
- Virginia Commonwealth University, USA Nov 2014

Locally Decodable and Updatable Non-Malleable Codes and Their Applications.

- University of Athens, Greece July 2014

Multi-input Functional Encryption.

- Eurocrypt, Denmark May 2014

Public-Key Cryptography from New Multivariate Quadratic Assumptions.

- Microsoft Research - Redmond, USA Jun 2012
- Public Key Cryptography, Darmstadt, Germany May 2012

Delegation in the Cloud.

- Brown Industrial Partners Program Symposium, USA Feb 2012

Tamper and Leakage Resilience in the Split-State Model.

- Crypto, Santa Barbara, USA Aug 2012
- NYU Theory Seminar, USA Nov 2011
- IBM TJ Watson Crypto Seminar, USA Nov 2011

Efficient String-Commitment from Weak Bit-Commitment.

- Asiacrypt, Singapore Dec 2010

Algorithmic Tamper-Proof Security Under Probing Attacks.

- Security and Cryptography for Networks (SCN), Italy Sep 2010

Fully Homomorphic Encryption Using Ideal Lattices.

- Seminar in Academia Sinica, Taiwan July 2009

Grants

CAREER: Towards Efficient Cryptography for Next Generation Applications, Active

Investigator: Feng-Hao Liu (Sole PI)
Total award amount: $500,000, roughly $260,000 transferred to WSU
Source of support: National Science Foundation (NSF)
Total award period covered: 10/1/2023 - 06/30/2025 (expected)
Location of project: Washington State University, WA

CAREER: Towards Efficient Cryptography for Next Generation Applications, Completed

Investigator: Feng-Hao Liu (Sole PI)
Total award amount: $500,000
Source of support: National Science Foundation (NSF)
Total award period covered: 07/01/2020 - 09/30/2023
Location of project: Florida Atlantic University, FL

CARES Funds, Completed

Investigator: Feng-Hao Liu (Co-PI)
My share: $103,031.43
Source of support: Florida Department of Education
Total award period covered: 07/01/2021 - 06/30/2022
Location of project: Florida Atlantic University, FL

CRII: SaTC: Practical Cryptographic Coding Schemes Against Memory Attacks, Completed

Investigator: Feng-Hao Liu (Sole PI)
Total award amount: $175,000
Source of support: National Science Foundation (NSF)
Total award period covered: 08/01/2017 - 07/31/2021 (no cost extension included)
Location of project: Florida Atlantic University, FL

Teaching and Advising

Courses Taught at WSU

Instructor, *EECS Department, Washington State University, WA*

- CPTS 580: Randomized Algorithm (New Course)
  Spring 2024
- CPTS 327: Introduction to Cybersecurity and Cryptography
  Spring 2024

Courses Taught at FAU

Instructor, *CEECS Department, Florida Atlantic University, FL*

- COT 6930: Computation Algorithms on Encrypted Data (New Course)
  Spring 2023
- COT 6930: Cryptography under Physical Attacks (New Course)
  Fall 2019, Spring 2021
- COT 6930/6446: Randomized Algorithms and Secure Designs (New Course)
  Fall 2015, Spring 2017, Fall 2018
- COT 6200: Philosophy of Computation (Redeveloped)
  Fall 2017
- EGN 4950C: RI: Engineering Design I
  Fall 2022
- EGN 4952C: RI: Engineering Design II
  Spring 2022

- COT 4930: Competitive Programming (New Course)
  Fall 2021
- STA 4821: Stochastic Models in CS
  Fall 2016, Spring 2017
- COT 4420: Formal Languages and Automata Theory
  Spring 2018, Summer 2018, Spring 2019, Spring 2020
- COP 3530: Data Structures and Algorithm Analysis
  Spring 2016, Fall 2016, Fall 2017, Spring 2018
- COP 2200: Introduction to Programming in C
  Summer 2016, Summer 2017
- COT 2000: Foundations of Computing (New Course)
  Spring 2022

Advising and Mentoring at WSU

Graduate Students

- Minzhang Li Ph.D., Started Spring 2024, in Progress
- Tianyu Zhao Ph.D., Started Spring 2024, in Progress

Advising and Mentoring at FAU

Postdoc

- Zhedong Wang July 2019 - June 2021
  First Job: Assistant Professor at Shanghai Jiao Tong University

Graduate Students

- Mohammad G. Raeini Ph.D., completed Aug 2022
  Co-advised with Mehrdad Nojoumian
  Thesis: Selected Applications of MPC
  First Job: Software Engineer at One Creation Corporation
- Zhedong Wang Ph.D., completed Jun 2019
  Co-advised at University of Chinese Academy of Sciences, China
  Thesis: Research on Lattice-based Public Key Cryptosystems Design and Tight Security
- Linir Zamir MS, completed Aug 2019
  Florida Atlantic University
  Thesis: Application of Blockchain Network for the Use of Information Sharing

Visiting Scholars

- Yun Song (Asooc Prof. at Shaanxi Normal University, China) Dec 2018 - Dec 2019
- En Zhang (Assoc Prof. at Henan Normal University, China) Nov 2018 - Nov 2019
- Qiqi Lai (Assoc Prof. Shaanxi Normal University, China) May 2018 - Apr 2019

- Chengbo Xu (Assoc Prof. Jinan University, China) Dec 2016 - Dec 2017

Thesis Committee

- Brian Koziel Ph.D., completed Aug 2022
  FAU, advisor Dr. Reza Azarderakhsh
- Rami El Khatib Ph.D., completed Aug 2022
  FAU, advisor Dr. Reza Azarderakhsh
- Ahmad Qutbuddin Ph.D., completed Aug 2022
  FAU, advisor Dr. Kwangsoo Yang
- Cole Hirapara MS, completed Dec 2019
  FAU, advisor Dr. Bassem Alhalabi
- Andrew Steinberg MS, completed Dec 2017
  FAU, advisor Dr. Mihaela Cardei

Services

External Professional Services

Panelist for National Science Foundation 2020 and 2024

- Reviewed and made recommendations for proposals in my field of expertise

Journal Editor 2021 - 2023

- IET Information Security

Program Committee Member Multiple years

- Asiacrypt 2023, Crypto 2023, CT-RSA 2023, Crypto 2022, ITC 2022, PKC 2022, PKC 2021, Asiacrypt 2020, Asiacrypt 2019, PKC 2019, Asiacrypt 2017, Asiacrypt 2016, AsiaPKC 2016, PKC 2016, International Workshop on Security in Cloud Computing (Asiaccs-SCC 2014), Information Security Conference (ISC 2014)

External Reviewer Multiple years

- Crypto, Eurocrypt, TCC, PKC, STOC, FOCS, Journal of Cryptology

Moderator at Strait Talk Symposium,Watson Institute, Brown U., RI. Oct 2012

- Moderated a discussion panel in the symposium about the topic: "Cyber-security and US-China-Taiwan Relations"

Internal Services

Student Competitions Advising 2021 - current

- Form and coach teams for programming competition

Department Undergraduate Committee 2017 - 2021

- Reviewing undergraduate courses, new proposals, and adjustments of programs

Department Instructor Search Committee Summer 2017

- Reviewed candidates of the instructor position, particularly in the technical level

Honors and Awards

FAU Junior Faculty Research Award	Feb 2021
NSF Career Award	July 2020
Selected as U.S. delegate to Heidelberg Laureate Forum via ORAU	Aug 2015
Best Student Paper Award of Theory of Cryptography Conference (TCC) 2010	Feb 2010
Google Fellowship, invited to Google Graduate Student Forum, CA, 2010	Jan 2010

Updated: February 8, 2024