(Jennie) Yu Zheng

3434 Engineering Hall, University of California, Irvine
☎ +1 (949) 795-xxxx ◇ ✉ yu.zheng@uci.edu ◇ Scholar ◇ Github

Future Work Authorization: Approved EB1A Visa (Priority Date: July 2023) for U.S. Permanent Resident.

CAREER PATH & EDUCATION

University of California, Irvine (UCI) *Sep 2024 - Present*
Postdoctoral Scholar, Department of Electrical Engineering & Computer Science. Irvine, US
Topic: Privacy-Preserving AI, LLM Privacy & Security.
Advisors: Zhou Li (Primary, UCI), Yupeng Zhang (Co-Advisor, UIUC).

Chinese University of Hong Kong (CUHK) *Aug 2018 - Jul 2024*
Doctor of Philosophy, Department of Information Engineering. Hong Kong SAR
Thesis: Communication-Efficient Protocols for Secure Training. Results: [C3],[M1], Productization.
Committee: Kehuan Zhang (Chair), Hongkai Chen, Haibo Hu (PolyU), Sze Ming Chow, Sze Yiu Chau.

Northeastern University (NEU) *Oct 2014 - Jun 2018*
Bachelor of Engineering, Department of Communication Engineering. Shenyang, CN
Thesis: Search over Encrypted Videos. Results: [C1],[J1]. Ranking: 1st of 96.

INTERNSHIPS & EXPERIENCE

University of California, San Diego & University of Utah *Mar 2024 - Apr 2025*
Visiting Research Assistant, Part-time. San Diego, US

· Mentor: Qingsong Wang. Topic: Graph Learning, Algebraic Topology.

Polytechnic University & Chinese University of Hong Kong *Aug 2024 - Sep 2024*
Interim Researcher, Full-time. Shatin, HKSAR

· Co-Advisors: Kai Zhou (PolyU, Financial), Kehuan Zhang (CUHK, Onsite).

Morse Team, Ant Group & Alibaba Group *May 2022 - Sep 2022*
Applied Research Intern - Algorithm, Full-time. Hangzhou, CN

· Mentor: Qizhi Zhang, Lichun Li. Topic: Private AI, Multiparty Computation, Number Theory.

Trustworthy Theory and Engineering Lab, 2012 Labs *Sep 2020 - Nov 2020*
Applied Research Intern - Security and Privacy, Full-time. Shenzhen, CN

· Mentor: Jiang Zhu. Topic: Secure Deep Learning, Multiparty Computation.

School of Computing, National University of Singapore *Jul 2018 - Aug 2018*
Summer School Participant, Full-time. Singapore

· Topic: Big Data, Cloud Computing.

Information Engineering, Chinese University of Hong Kong *Mar 2018 - May 2018*
Research Assistant, Full-time. Shatin, HKSAR

· Mentor: Minxin Du. Topic: Searchable Encryption.

SELECTED AWARD

Travel Grant for NSF NeTS Early-Career Investigators Workshop.	2025
Conference Travel Award of IEEE SaTML, UToronto, Canada.	2024
Summer Research Institute Fellowship of EPFL, Switzerland (1 of 20).	2023
ACM MMSys Best Student Paper Award (1st Authorship).	2022

Bachelor Dissertation Award (Top 1%).	2018
Outstanding Bachelor's Graduate of Liaoning Division, China (Top 3%).	2017
ICCT Best Paper Award.	2017
Honorable Mention of American Mathematical Contest in Modeling.	2017
Second Prize of Chinese (National) Undergraduate Mathematical Contest in Modeling.	2016
National Scholarship of China ×2 (Top 0.2%).	2016/2015
Third Prize of National Undergraduate Competition on Information Security, China.	2016
Outstanding Student Leader for Social Practice at NEU, China (Top 3%).	2015
Outstanding Student of Northeastern University for Academic Excellence, China.	2017/2016/2015

SELECTED PUBLICATIONS & PREPRINTS

Citations: 654; h-index: 11; i10-index: 12; As of Oct 2025. [Full List]

arXiv Manuscripts († for co-first authorship, # for alphabetical order)

[M3] Danyu Sun, Jinghuai Zhang, Jiacen Xu, **Yu Zheng**, Yuan Tian, and Zhou Li. "From Alerts to Intelligence: A Novel LLM-Aided Framework for Host-based Intrusion Detection." [arXiv]

[M2] **Yu Zheng**, Chenang Li, Zhou Li, and Qingsong Wang. "Convergent Privacy Framework with Contractive GNN layers for Multi-hop Aggregations." Under Major Revision of Network and Distributed System Security Symposium (NDSS), 2026.

[M1] **Yu Zheng†**, Qizhi Zhang†, Chenang Li, Lichun Li, Kai Zhou, and Shan Yin. "Secure Graph Convolutional Network on Vertically Split Data from Sparse Matrix Decomposition." Preliminary version accepted in Deep Learning Security and Privacy Workshop co-located with the IEEE Symposium on Security and Privacy, 2025. [Poster] [arXiv]

Conference

[C7] Jiacen Xu, Chenang Li, **Yu Zheng**, and Zhou Li. "Entente: Cross-silo Intrusion Detection on Network Log Graphs with Federated Learning." Network and Distributed System Security Symposium (NDSS), 2026. [Code]

[C6] Xiuhua Wang, Shikang Li, Fengrui Fan, Shuai Wang, Yiwei Li, and **Yu Zheng**. "Improving Byzantine-resilience in Federated Learning via Diverse Aggregation and Adaptive Variance Reduction." International Conference on Information and Communications Security (ICICS), 2025.

[C5] Xiangfu Song, **Yu Zheng**, Jianli Bai, Changyu Dong, Zheli Liu, and Ee-Chien Chang. "DISCO: Dynamic Searchable Encryption with Constant State." ACM Asia Conference on Computer and Communications Security (AsiaCCS), 2024. [Code]

[C4] Zhiqin Yang, Yonggang Zhang, **Yu Zheng**, Xinmei Tian, Hao Peng, Tongliang Liu, and Bo Han. "FedFed: Feature Distillation against Data Heterogeneity in Federated Learning." Advances in Neural Information Processing Systems (NeurIPS), 2023. [Code]

[C3] **Yu Zheng†**, Qizhi Zhang†, Sherman S.M. Chow, Yuxiang Peng, Sijun Tan, Lichun Li, and Shan Yin. "Secure Softmax/Sigmoid for Machine-Learning Computation." Annual Computer Security Applications Conference (ACSAC), 2023. [Code] [Slides]

[C2] **Yu Zheng**, Wei Song, Minxin Du, Sherman S.M. Chow, Qian Lou, Yongjun Zhao, Xiuhua Wang. "Cryptography-Inspired Federated Learning Variants for GAN and Meta Learning." International Conference on Advanced Data Mining and Applications (ADMA), 2023. [Code] [Slides]

[C1] **Yu Zheng**, Heng Tian, Minxin Du, and Chong Fu. "Encrypted Video Search: Scalable, Modular, and Content-similar." ACM Multimedia Systems Conference (MMSys), 2022. (***Best Student Paper Award***) [Code] [Slides]

Journal

[J2] Xing Ai, Yulin Zhu, **Yu Zheng**, Gaolei Li, Jianhua Li, and Kai Zhou. "Revisiting Adversarial Robustness of GNNs against Structural Attacks: a Simple and Fast Approach." Transactions on Information Forensics & Security (TIFS), 2025.

[J1] **Yu Zheng**, Wenchao Zhang, Wei Song, Xiuhua Wang, and Chong Fu. "Encrypted Video Search with Single/Multiple Writers." ACM Transactions on Multimedia Computing, Communications, and Applications, 2024. (Invited Submission)

RESEARCH GRANTS & PROPOSALS

· "Collaborative Research: PDaSP: Track 1: Practical Secure Multiparty Computations for Graph-based Intrusion Detection Systems." from **NSF**, 2025 - 2027. (**Grant: $750K**) I contributed core techniques [M1] and drafted the proposal with two advisors. I am mentoring a new PhD student for [N1].
Co-PIs: Zhou Li (UC Irvine), Yupeng Zhang (UIUC). Senior Personnel

· "Efficient Privacy-Enhancing Techniques for Edge Computing." from NSF NeTS Early-Career Investigators Workshop, 2025. (Travel Grant: ≈$1K) Investigator

· "Secret Communications through Steganography and Chaotic Encryption." from NEU Key Program for Undergraduate Research Training, 2016 - 2017. (Award: ¥86K≈$13K) Team Leader

PROFESSIONAL SERVICE

Organizing Committee:
(*26'*): Publicity Chair for PRISM Workshop co-located with NDSS. San Diego

Program Committee:
(*26'*): ACM CCS.
(*25'*): ACSAC, AAAI, ACNS-SiMLA, ACM WPES@CCS, ICNC.
(*24'*): CCS AE, NDSS AE (Discussion Lead), TheWebConf AE, USENIX Security AE, EAI ICECI.
(*23'*): CCS AE, AJCAI.

Session Chair/Host:
(*25'*): S&P (San Francisco), RSA (San Francisco), NDSS (San Diego).
(*24'*): AsiaCCS (Singapore).

Review Service:
ICLR. (*26'*)
ACM TOPS, ICLR, ICML, NeurIPS, TMLR, TDSC. (*25'*)
AISTATS, AsiaCCS, ICLR, ICML, IEEE TDSC, Information Sciences, NeurIPS. (*24'*)
Information Sciences, NCAA, NeurIPS, JMANS. (*23'*)

TEACHING SERVICE

Mentoring:
Chenang Li, PhD@UCI (Advisors: Zhou Li@UCI, Yupeng Zhang@UIUC) Oct 2024 - Aug 2025
Topic: System Security, Secure Graph Learning. Result: [N1].

Guest Lectures:
EECS231(by Zhou Li)@UCI: MPC Protocols for Sparse Graph Computations. Feb 2025
CAP6614(by Qian Lou)@UCF: Secure Machine Learning with Multiparty Computation. Feb 2024

Teaching Assistant Courses:
Introduction to Cyber Security. Spring 2020, Spring 2019

Web Programming and Security.	Spring 2021, Fall 2019
Electronic Circuit Design Lab.	Fall 2021, Fall 2020, Fall 2018
Microcontroller and Embedded Systems Lab.	Spring 2022, Fall 2022
Technology Strategy and Commercialization.	Spring 2024
Introduction to Microcontroller.	Summer 2015

TALKS & PRESENTATION

(Poster): Secure GCN on Vertically Split Data.	GEECS Annual Technology Showcase, Jun 2025
(Poster): Secure Graph Convolutional Network on Vertically Split Data.	DLSP@S&P, May 2025
(Seminar): Secure Graph Convolutional Network on Vertically Split Data.	ICS@UCI, Feb 2025
(Pitch): Practical Privacy-Enhancing Techniques for Edge Computing.	NeTS@NSF, Jan 2025
(Talk): Secure Graph Convolutional Network on Vertically Split Data.	ECE@VirginiaTech, Jan 2025
(Seminar): Secure Graph Convolutional Network on Vertically Split Data.	CS@UMD, Jan 2025
(Poster): Secure Graph Convolutional Network on Vertically Split Data.	WiCyS@UCI, Nov 2024
(Seminar): Efficient MPC Protocols for Secure Machine Learning.	CSE@UCSC, Apr 2024
(Conference): Secure Softmax/Sigmoid for Machine-Learning Computation.	ACSAC, Dec 2023
(Oral/Conference): Cryptography-Inspired Federated Learning Variants.	ADMA/NEU, Aug 2023
(Poster): Secure Softmax/Sigmoid for Machine-Learning Computation.	EPFL, Jul 2023