(Jennie) Yu Zheng

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

I will be on job market for a research position in 2025 Fall.
Work Authorization: Approved EB1A Visa (PD in 2023).

CAREER PATH & EDUCATION

University of California, Irvine *Sep 2024 - Present*
Postdoctoral Scholar, Department of Electrical Engineering & Computer Science. Irvine,US
Topic: Secure AI, AI for Security, Privacy, System Security.
Advisor: Zhou Li.

Chinese University of Hong Kong *Aug 2018 - Jul 2024*
Doctor of Philosophy, Department of Information Engineering. Hong Kong SAR
Thesis: Communication-Efficient Protocols for Secure Training. Results: [C4],[M3], Productization.
Committee: Kehuan Zhang (Chair), Hongkai Chen, Haibo Hu, Sze Ming Chow, Sze Yiu Chau.

Northeastern University *Oct 2014 - Jun 2018*
Bachelor of Engineering, Department of Communication Engineering. Shenyang,CN
Thesis: Search over Encrypted Videos. Results: [C2],[J8]. Ranking: 1st of 96.

RESEARCH INTERESTS

Secure Machine Learning: Cryptography with Learning, Private Graph Learning, Differential Privacy, LLM Privacy, Medical Privacy.
Cryptography & Cybersecurity: Multiparty Computation, Zero-Knowledge Proof, Steganography, Network Intrusion Detection, Security Analytics.

I am broadly interested into mathematics, physics, economics, psychology, and sociology.

WORKING HISTORY

University of California, San Diego & University of Utah *Mar 2024 - Apr 2025*
Visiting Research Assistant, Part-time. San Diego/Remote,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).
· Topic: Differential Privacy and Adversarial Robustness for Trustworthy Graph Learning.

Information Engineering, Chinese University of Hong Kong *Aug 2018 - Mar 2024*
Teaching Assistant, Part-time. Shatin,HKSAR
· Teaching: Cryptography, Security, Circuits, Embedded System, Research, Products Commercialization.

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.
· Results: [C4], 6 Patents for Algorithms, 2 Commercial Products.

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 Software, Shandong University *Nov 2019 - Jan 2020*
Visiting Research Assistant, Full-time. Jinan,CN

· Advisor: Qiuliang Xu. Mentor: Xiangfu Song. Topic: Applied Cryptography. Result: [C6].

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

· Mentor: Minxin Du. Topic: Searchable Encryption. Result: [C2].

Information Security Laboratory, Northeastern University *Dec 2015 - June 2018*
Research Assistant, Part-time. Shenyang,CN

· Advisor: Chong Fu. Topic: Chaotic Encryption, Parallel Computing. Results: [C1],[J1]-[J4].

Electronic Engineering Laboratory, Northeastern University *Dec 2014 - Aug 2015*
Student Technician, Part-time. Shenyang,CN

· Technician: Dayu Li. Topic: Circuit, Microcontroller, Intelligent Vehicle, Quadrotor.

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
CUHK Postgraduate Scholarship, Hong Kong SAR.	2018
Outstanding Bachelor's Graduate of Liaoning Division, China (Top 3%).	2017
ICCT Best Paper Award.	2017
Travel Grant for SAKURA Exchange Program in Science, Japan.	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 $\times 2$ (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
Second Prize of Undergraduate Electronic Design Contest in Liaoning Division, China.	2015
Outstanding Student of Northeastern University for Academic Excellence, China.	2017/2016/2015
Merit Freshman of Northeastern University, China (Top 1%).	2014

PUBLICATIONS

Citations:520; h-index:11; i10-index:11; As of May 2025

I enjoy learning new knowledge, and am always open to collaboration or technical discussion.

Conference *(† for co-first authorship)*

[C6] 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. (CORE-A)

[C5] 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. (CORE-A*)

[C4] **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. [Available Badge, Functional Badge, Reproduced Badge] (CORE-A)

[C3] **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. (Oral; CORE-B)

[C2] **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***)

[C1] Chong Fu, **Yu Zheng**, Min Chen, and Zhankao Wen. "A Color Image Encryption Algorithm Using A New 1-D Chaotic Map." International Conference on Communication Technology (ICCT), 2017. (***Best Paper Award***)

Journal

[J10] Wei Song, Chong Fu, **Yu Zheng**, Junxin Chen, and Yanfeng Zhang. "Neural Network-driven Parallel Accelerated Selective Image Encryption with Semantic Understanding." The European Physical Journal Special Topics, 2025.

[J9] Yuxiang Peng, Chong Fu, **Yu Zheng**, Yunjia Tian, Guixing Gao, and Junxin Chen. "Medical Steganography: Enhanced Security and Image Quality, and New S-Q Assessment." Signal Processing, 2024. (JCR-Q2, IF:4.40)

[J8] **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; JCR-Q1, IF:5.63)

[J7] Wei Song, Chong Fu, **Yu Zheng**, Yanfeng Zhang, Junxin Chen, and Peipei Wang. "Batch Image Encryption Using Cross Image Permutation and Diffusion." Journal of Information Security and Applications, 2024. (JCR-Q2, IF:4.96)

[J6] Haoyu Xie, Chong Fu, Xu Zheng, **Yu Zheng**, Chiu-Wing Sham and Xingwei Wang. "Adversarial Co-Training for Semantic Segmentation over Medical Images." Computers in Biology and Medicine, 2023. (JCR-Q1, IF:6.98)

[J5] Wenchao Zhang, Chong Fu, **Yu Zheng**, Fangyuan Zhang, and Chiu-Wing Sham. "HSNet: A Hybrid Semantic Network for Polyp Segmentation." Computers in Biology and Medicine, 2022. (JCR-Q1, IF:6.98)

[J4] Wei Song, Chong Fu, **Yu Zheng**, Ming Tie, Jun Liu, and Junxin Chen. "A Parallel Image Encryption Algorithm Using Intra Bitplane Scrambling." Mathematics and Computers in Simulation, 2023. (JCR-Q2, IF:3.81)

[J3] Wei Song, Chong Fu, **Yu Zheng**, Lin Cao, and Ming Tie. "A Practical Medical Image Cryptosystem with Parallel Acceleration." Journal of Ambient Intelligence and Humanized Computing, 2022. (JCR-Q1, IF:7.10)

[J2] Wei Song, Chong Fu, **Yu Zheng**, Lin Cao, Ming Tie, and Chiu-Wing Sham. "Protection of Image ROI Using Chaos-based Encryption and DCNN-based Object Detection." Neural Computing and Applications, 2022. (JCR-Q1, IF:5.60)

[J1] Wei Song, **Yu Zheng**, Chong Fu, and Pufang Shan. "A Novel Batch Image Encryption Algorithm Using Parallel Computing." Information Sciences, 2020. (JCR-Q1, IF:6.70)

arXiv Manuscripts

[M4] Jiacen Xu, Chenang Li, **Yu Zheng**, and Zhou Li. "Entente: Cross-silo Intrusion Detection on Network Log Graphs with Federated Learning". `https://arxiv.org/pdf/2503.14284`

[M3] **Yu Zheng**†, Qizhi Zhang†, Lichun Li, Kai Zhou, and Shan Yin. "Secure Graph Convolutional Network on Vertically Split Data from Sparse Matrix Decomposition." `https://arxiv.org/pdf/2502.09808` (Preliminary version accepted as extended abstract in DLSP@S&P'25)

[M2] **Yu Zheng**, Wenchao Zhang, Yonggang Zhang, Wei Song, Kai Zhou, and Bo Han. "Revisiting Privacy-Utility Trade-off for DP Training with Pre-existing Knowledge." arXiv:2409.03344.

[M1] Xing Ai, Guanyu Zhu, Yulin Zhu, **Yu Zheng**, Gaolei Li, Jianhua Li, and Kai Zhou. "SFR-GNN: Simple and Fast Robust GNNs against Structural Attacks." arXiv:2408.16537.

Code*&*Artifacts

[A6] Github Repo for "Batch Image Encryption using Cross Image Permutation and Diffusion." (JISA'24)

[A5] Github Repo for "FedFed: Feature Distillation against Data Heterogeneity in FL." (NeurIPS'23)

[A4] Github Repo for "Secure Softmax/Sigmoid for Machine-Learning Computation." (ACSAC'23)

[A3] Github Repo for "Cryptography-Inspired FL Variants for GAN and Meta Learning." (ADMA'23)

[A2] Github Repo for "HSNet: A Hybrid Semantic Network for Polyp Segmentation." (CIBM'22)

[A1] Github Repo for "Encrypted Video Search: Scalable, Modular, and Content-similar." (MMSys'22)

RESEARCH GRANTS & PROPOSALS

Principal Contributor & Leader:

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

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

Co-Writer as Trainee or Helper:

(Pray) ...

Training Programs Attended:
Federal Grant Programs for Early – Career Investigators. McAllister&Quinn, Mar 2025
DARPA's Defense Sciences Office – Chasing the (Near) Impossible. DARPA, Feb 2025

PROFESSIONAL SERVICE

I am glad to contribute and support our community.

Program Committee:
(*25'*): ACSAC, AAAI, ACNS-SiMLA, 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'25 (San Francisco), NDSS (San Diego).
(*24'*): AsiaCCS (Singapore).

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

Information Sciences, NCAA, NeurIPS,JMANS. (*23'*)
TVCJ. (*22'*)

External: AsiaCCS (19'), CRYPTO (19'), ESORICS (19'), ICICS (19'), IEEE S&P (25'), IEEE TIFS (19'), ISC (19'), NDSS (26',25'), RAID (23'), SecureComm (19',18'), TheWebConf (23',20'), ...

TEACHING SERVICE

(*I am happy to support and work with students, usually through thesis, course, or exam.*)

Mentoring:

Chenang Li, PhD@UCI (Adviser: Zhou Li) Oct 2024 - Present
Topic: Security.

Yitian Cheng, Visiting@UCI (Adviser: Zhou Li) → Master@ZJU Jul 2024 - May 2025
Topic: Federated Learning.

Yuxiang Peng, PhD@NEU (Adviser: Chong Fu) Apr 2023 - May 2024
Topic: AI for Information Hiding, Steganography. Result: [J9], etc.

Andes Y.L. Kei, PhD@CUHK May 2023 - Oct 2023
Topic: Secure Machine Learning, Multiparty Computation.

Zhiqin Yang, RA@HKBU (Advisors: Bo Han, Yonggang Zhang) → PhD@CUHK Aug 2022 - Mar 2023
Topic: Federated Learning, Differential Privacy. Result: [C5].

Zheng Yang, MSc@CUHK → Engineer@ByteDance Sep 2021 - Dec 2021
Topic: Privacy-Preserving Deep Learning, Differential Privacy.

Heng Tian, MEng@NEU (Adviser: Chong Fu) → Engineer@AICC Nov 2020 - May 2022
Topic: Searchable Encryption on Multimedia. Result: [C2].

Xiang Li, MSc@CUHK → PhD@UTokyo Sep 2019 - Apr 2020
Topic: Privacy-Preserving Deep Learning, Differential Privacy.

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

Training Programs Attended:

Improv For Teaching Certificate Program. UCI, 2025
Presentation Skills & Teaching, and Communication Workshops. CUHK, 2019

TALKS & PRESENTATION

(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

DIVERSITY & INCLUSION

Presenter and Attendee @ Women in Cybersecurity, UCI. Nov 2024

ACADEMIC ATTENDANCE

Conference & Workshops:

NDSS@San Diego, RSA@San Francisco, S&P(&DLSP)@San Francisco, SoCal Security@Riverside, TPDP@San Francisco. 2025
HotNets@Irvine, AsiaCCS@Singapore, SaTML@Toronto,CA. 2024
ADMA@Shenyang,CN, ACSAC@Austin. 2023
MMSys@Virtual. 2022
CRYPTO@Virtual. 2020

Schools & Programs:

Summer Research Institute @EPFL, CH. (Topic: Systems, Security, and Privacy) Jul 2023 - Jul 2023
Crypto Summer School @ZJU, CN. (Topic: Provable Security) Jun 2023 - Jul 2023
ACE-SIP Summer School @MonashUniv, AU. (Topic: Blockchain) Feb 2023 - Feb 2023
Summer School @NUS, Singapore. (Topic: Big Data, Cloud Computing) Jul 2018 - Aug 2018
Summer School @TUT, JP. (Topic: Virtual Reality, Intelligent Vehicle) Jul 2017 - Jul 2017

SOCIAL SERVICE

Volunteer for Funeral of Sir Charles Kuen Kao. Oct 2018
Host of "Sangfor" National Elite Competition in Liaoning Division. Aug 2017
Volunteer for National Undergraduate Electronic Design Contest. Aug 2015
Volunteer for National Undergraduate Information Security Competition. Aug 2015
Ritual Girl for Graduation Party. May 2015
Committee Member of Class. 2014-2018
Class President. 2009-2014
Basketball Starting Lineup of School Team (Point Guard). 2009-2011

LANGUAGE

Mandarin (Native), English (Fluent), Cantonese (Medium), C, C++, Python, Matlab, R, Java, LaTeX, HTML, CSS, JavaScript, ...