(Jennie) Yu Zheng

SHB 726, Chinese University of Hong Kong, Shatin, Hong Kong SAR
(+852) 6955-0625 ◇ yuzheng404@link.cuhk.edu.hk ◇ Scholar ◇ Github

CAREER PATH & EDUCATION

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

Polytechnic University & Chinese University of Hong Kong *Aug 2024 - Sep 2024*
Interim Researcher, Department of Computing (PolyU) & Information Engineering (CUHK).
Topic: Differential Privacy and Adversarial Robustness for Trustworthy Graph Learning.
Co-Advisors: Kai Zhou (PolyU, Financial), Kehuan Zhang (CUHK, Onsite).

Chinese University of Hong Kong, Hong Kong SAR *Aug 2018 - Jul 2024*
Doctor of Philosophy, Department of Information Engineering.
Thesis: Communication-Efficient Protocols for Secure Training. Results: [C4], Productization.
Co-Advisors: Sherman S.M. Chow (Academic/Official), Qizhi Zhang (Industrial/External).

Northeastern University, Shenyang, CN *Oct 2014 - Jun 2018*
Bachelor of Engineering, Department of Communication Engineering, Ranking: 1^{st} of 96.
Thesis: Search over Encrypted Videos. Results: [C2],[J2].
Co-Advisors: Chong Fu (Official), Sherman S.M. Chow (External).

RESEARCH INTERESTS

Secure Machine Learning. [C3,C4] via Crypto, [C5] via DP.
- Cryptography with Learning, Differential Privacy, Medical Privacy. [Research Topics]

Applied Cryptography. [C2,C6,J2] for SE.
- Multiparty Computation, Zero-Knowledge Proof, Encryption, Steganography. [Study Interests]

Miscellaneous. Mathematics, Physics, Economics, Psychology, Sociology. [Sparetime]

SELECTED PUBLICATION

Citations: 337; h-index:9; i10-index-7; As of Sep 2024

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

[J3] 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)

[J2] **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)

[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)

SELECTED AWARD

Conference Travel Award of IEEE SaTML, UToronto, Canada (Amount: 3.5K USD)	2024
Summer Research Institute Fellowship of EPFL, Switzerland (1 of 20, Amount: 500 CHF)	2023
ACM MMSys Best Student Paper Award (1^{st} Authorship, Amount: 750 EUR)	2022
Outstanding Research Project for NEU Bachelor's Degree (Top 1%)	2018
CUHK Postgraduate Scholarship	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 $\times 2$ (Top 0.2%, 8K CNY $\times 2$)	2016/2015
Third Prize of National Undergraduate Competition on Information Security	2016
Outstanding Student Leader for Social Practice at NEU, China (Top 3%)	2015
Second Prize of Undergraduate Electronic Design Contest in Liaoning Division	2015
Outstanding Student of Northeastern University for Academic Excellence	2017/2016/2015
Merit Freshman of Northeastern University (Top 1%)	2014

PROGRAM COMMITTEE

CCS AE (24',23'), NDSS AE (24', also Discussion Lead in 24'), TheWebConf AE (24'), USENIX Security AE (24'), AAAI (25'), AJCAI (23'), EAI ICECI (24'), ICNC (25').

(24'): Session Chair of AsiaCCS.

REVIEW SERVICE

Cryptography (Official): AsiaCCS (24'), IEEE TDSC (24'), IEEE TSC (24'), Information Sciences (24',23')
Learning (Official): AISTATS (24'), ICLR (24'), ICML (24'), NeurIPS (24',23'), NCAA (23'), TVCJ (22'), JMANS (23')
Cryptography (External): AsiaCCS (19'), CRYPTO (19'), ESORICS (19'), ICICS (19'), IEEE S&P (25'), IEEE TIFS (19'), ISC (19'), NDSS (25'), RAID (23'), SecureComm (19',18'), TheWebConf (23',20')

TEACHING SERVICE

Courses: Introduction to Cyber Security (S20,S19), Web Programming and Security (S21,F19), Electronic Circuit Design Lab (F21,F20,F18), Microcontroller and Embedded Systems Lab (S22,F22), Technology Strategy and Commercialization (S24).

Mentees:

Chenang Li, PhD@UCI (Advised by Zhou Li) — Oct 2024 - Present
Topic: System Security, MPC, Graph Learning.

Yitian Cheng, Intern@UCI (Advised by Zhou Li) — Jul 2024 - Present
Topic: Federated Learning, Security.

Yuxiang Peng, PhD@NEU (Advised by Chong Fu) — Apr 2023 - May 2024
Topic: AI for Information Hiding, Steganography. Result: [J3].

Andes Y.L. Kei, PhD@CUHK (Advised by Sherman Chow) — May 2023 - Oct 2023
Topic: Secure Machine Learning, Multiparty Computation.

Zhiqin Yang, MEng@BUAA → PhD@CUHK (Co-Mentored with Yonggang) — Aug 2022 - Mar 2023
Topic: Federated Learning, Differential Privacy. Result: [C5].

Zheng Yang, MSc@CUHK → Engineer@ByteDance (Advised by Sherman Chow) — Sep 2021 - Dec 2021
Topic: Privacy-Preserving Deep Learning, Differential Privacy.

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

Xiang Li, MSc@CUHK → PhD@UTokyo (Advised by Sherman Chow) — Sep 2019 - Apr 2020
Topic: Privacy-Preserving Deep Learning, Differential Privacy.

TALKS & LECTURE

(Seminar): Efficient MPC Protocols for Secure Machine Learning. — CSE@UCSC, Apr 2024
(Guest Lecture): Secure Machine Learning with Multiparty Computation. — CAP6614/UCF, Feb 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 s cho

WORKING EXPERIENCE

Mathematics Department, University of Utah — *Mar 2024 - Aug 2024*
Visiting Research Assistant, Part-time — Remote/Salt Lake,US
· Mentor: Qingsong Wang. Topic: Graph Learning, Algebraic Topology.

Information Engineering, Chinese University of Hong Kong — *Aug 2018 - Mar 2024*
Teaching Assistant, Part-time — Shatin,HK
· 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: Secure Machine Learning, Multiparty Computation.
· Results: [C4], 6 Chinese 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].

Cryptography Group, Chinese University of Hong Kong *Mar 2018 - May 2018*
Research Assistant, Full-time Shatin,HK

· Advisor: Sherman S.M. Chow. 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], etc.

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

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

ACADEMIC ATTENDANCE

Secure and Trustworthy Machine Learning Conference @UToronto Apr 2024 - Apr 2024
Topic: Trustworthy AI, Differential Privacy, Secure ML. (with Travel Award) Toronto,CA

Summer Research Institute @EPFL Jul 2023 - Jul 2023
Topic: Systems, Security, and Privacy. (with SuRI Fellowship) Lausanne,CH

Crypto Summer School @Zhejiang University Jun 2023 - Jul 2023
Host: Chinese Association for Cryptologic Research. Topic: Provable Security. Hangzhou,CN

ACE-SIP Summer School @Monash University Feb 2023 - Feb 2023
Topic: Blockchain and Algorand Ecosystem. (with Travel Stipend) Melbourne,AU

Summer School @National University of Singapore Jul 2018 - Aug 2018
Topic: Big Data, Cloud Computing. Singapore

Summer School @Toyohashi University of Technology Jul 2017 - Jul 2017
Topic: Virtual Reality, Intelligent Vehicle. (with Travel Stipend) Toyohashi,JP

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

LANGUAGE

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