Minxin Du

Research Assistant Professor
Department of Electrical and Electronic Engineering
The Hong Kong Polytechnic University

Mobile: (+852) 5423 9412
Email: minxin.du@polyu.edu.hk
Website: https://duminxin.github.io

Research Interests

- Differential Privacy (New Notions and Applications to Large Language Models)
- Applied Cryptography (*e.g.*, Searchable/Graph Encryption, Information Retrieval)
- Privacy-preserving Machine (Un)Learning
- Secure Outsourcing or Multi-party Computation

Professional Experience

The Hong Kong Polytechnic University — Hong Kong, China
Research Assistant Professor — 07/2024-present

The Chinese University of Hong Kong — Hong Kong, China
Research Associate/Post-doc — 11/2023-06/2024

Education

The Chinese University of Hong Kong — **Advisor: Sherman S. M. Chow**
Ph.D., Department of Information Engineering — 08/2018-10/2023
Thesis: *Differential Privacy for Text Analytics via Forward-Pass Signal Sanitization*
Committee Members: *Yingjun (Anglea) Zhang (chair), Ashwin Machanavajjhala (external examiner), Xiaojun Lin, CheukTing Li, and Sherman S. M. Chow*

Wuhan University — **Advisor: Qian Wang**
M.Eng., Information Security — 09/2015-06/2018

Wuhan University — **Advisor: Qian Wang**
B.Eng., Computer Science and Technology — 09/2011 - 07/2015
HongYi (from university motto) Elite Class — GPA: 3.52/4.0, Rank: top 10%

Honors and Awards

- EPFL Summer Research Institute (SuRI) Ph.D. Fellowship (Jul. 2023, Bonus: 500 CHF)
- Best Student Paper Award, ACM MMSys 2022 (Bonus: 750 EUR)
- Outstanding Teaching Assistant Award (2nd Term, 2020-2021, Bonus: 1,000 HKD)
- Postgraduate Second-class Academic Innovation Award (2019) (Bonus: 15,000 RMB)
- Student Stipend for Crypto Innovation School (Dec. 2018, Bonus: 500 USD)
- Scholarship of Cyber Security, China Internet Development Foundation (Bonus: 50,000 CNY)
- Postgraduate National Scholarship (2017-2018) (Top 24 out of 344, Bonus: 20,000 CNY)
- China Graduate Contest on Application, Design and Innovation of Mobile-Terminal. First Prize (Oct. 2016) (Rank top 8 out of 160 teams in the final contest)
- Honor Graduate Award of HongYi Class (Jun. 2015)

Research Grants

1. "Privacy Enhancing Technologies for Large (Language) Models", **PolyU Start-up Fund**, 2024.08-2026.08, **PI**. (Amount: 300,000 HKD)

Publications

As of Feb. 2025, Google Scholar citations: **1001** with **h-index 16**.

Refereed Conferences Papers (in chronological order)
$*$: Equal contribution, #: Corresponding author

1. Jin Yao, Eli Chien, **Minxin Du**, Xinyao Niu, Tianhao Wang, Zezhou Cheng, and Xiang Yue. "Machine Unlearning of Pre-trained Large Language Models". *pp. 8403–8419.* ACL'24 (CCF-A)
2. **Minxin Du**, Xiang Yue*, Sherman S. M. Chow, Tianhao Wang, Chenyu Huang, and Huan Sun. "DP-Forward: Fine-tuning and Inference on Language Models with Local Differential Privacy in Forward Pass". *pp. 2665-2679.* ACM CCS '23 (CCF-A)
3. **Minxin Du**, Xiang Yue, Sherman S. M. Chow, Huan Sun. "Sanitizing Sentence Embeddings (and Labels) for Local Differential Privacy". *pp. 2349-2359.* ACM TheWebConf '23 (CCF-A)
4. Yu Zheng, Wei Song, **Minxin Du**, Sherman Chow, Qian Lou, and Xiuhua Wang. "Cryptography-Inspired Federated Learning for Generative Adversarial Networks and Meta Learning". *pp. 393-407.* ADMA '23 (CCF-C)
5. Yu Zheng, Heng Tian, **Minxin Du**$^{\#}$, and Chong Fu. "Sanitizing Sentence Embeddings (and Labels) for Local Differential Privacy". *pp. 177-190.* ACM MMSys '22 (**Best Student Paper**)
6. Xiang Yue, **Minxin Du***, Tianhao Wang, Yaliang Li, Huan Sun, and Sherman S. M. Chow. "Differential Privacy for Text Analytics via Natural Text Sanitization". *pp. 3853-3866.* Findings of ACL '21 (CCF-A)
7. Jiafan Wang, **Minxin Du***, and Sherman S. M. Chow. "Stargazing in the Dark: Secure Skyline Queries with SGX". *pp. 322-338.* DASFAA '20 (CCF-B)
8. Minghui Li, Mingxue Zhang, Qian Wang, Sherman S. M. Chow, **Minxin Du**, Yanjiao Chen, and Chenliang Li. "InstantCryptoGram: Secure Image Retrieval Service". *pp. 2222-2230.* INFOCOM '18 (CCF-A)
9. Qian Wang, Kui Ren, **Minxin Du**, Qi Li, and Aziz Mohaisen. "SecGDB: Graph Encryption for Exact Shortest Distance Queries with Efficient Updates". *pp. 79-97.* FC '17 (CCF-C)
10. Qian Wang, Shengshan Hu, **Minxin Du**, Jingjun Wang, and Kui Ren. "Learning Privately: Privacy-Preserving Canonical Correlation Analysis for Cross-Media Retrieval". *pp. 1-9.* INFOCOM '17 (CCF-A)
11. Qian Wang, Shengshan Hu, Kui Ren, Jingjun Wang, Zhibo Wang, and **Minxin Du**. "Catch Me in the Dark: Effective Privacy-preserving Outsourcing of Feature Extractions over Image Data". *pp. 1-9.* INFOCOM '16 (CCF-A)
12. Qian Wang, Shengshan Hu, Kui Ren, Meiqi He, **Minxin Du**, and Zhibo Wang. "CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud". *pp. 186-205.* ESORICS'15 (CCF-B)

Refereed Journal Papers (in chronological order)

1. Man Zhou, Wenyu Zhou, Jie Huang, Junhui Yang, **Minxin Du**$^{\#}$, Qi Li. "Stealthy and Effective Physical Adversarial Attacks in Autonomous Driving". *IEEE Transactions on Information Forensics and Security (TIFS), 19: 6795-6809, 2024 (CCF-A).*
2. Xiaoxue Hu, Geling Liu, Baolin Zheng, Lingchen Zhao, Qian Wang, Yufei Zhang, **Minxin Du**. "FastTextDodger: Decision-Based Adversarial Attack Against Black-Box NLP Models With Extremely High Efficiency". *IEEE Transactions on Information Forensics and Security (TIFS), 19: 2398-2411, 2024 (CCF-A).*
3. Yunjie Ge, Lingchen Zhao, Qian Wang, Yiheng Duan, and **Minxin Du**. "AdvDDoS: Zero-query Adversarial Attacks Against Commercial Speech Recognition Systems". *IEEE Transactions on Information Forensics and Security (TIFS), 18: 3647-3661, 2023 (CCF-A).*

4. **Minxin Du**, Peipei Jiang, Qian Wang, Sherman S. M. Chow, and Lingchen Zhao. "Shielding Graph for eXact Analytics with SGX". *IEEE Transactions on Dependable and Secure Computing (TDSC), 20(6): 5102-5112, 2023 (CCF-A).*
5. **Minxin Du**, Shuangke Wu, Qian Wang, Dian Chen, Peipei Jiang, and Aziz Mohaisen. "GraphShield: Dynamic Large Graphs for Secure Queries with Forward Privacy". *IEEE Transactions on Knowledge and Data Engineering (TKDE), 34(7): 3295-3308, 2020 (CCF-A).*
6. **Minxin Du**, Qian Wang, Meiqi He, and Jian Weng. "Privacy-preserving Indexing and Query Processing for Secure Dynamic Cloud Storage". *IEEE Transactions on Information Forensics and Security (TIFS), 13(9): 2320-2332, 2018 (CCF-A).*
7. Qian Wang, **Minxin Du**, Xiuying Chen, Yanjiao Chen, Pan Zhou, Xiaofeng Chen, and Xinyi Huang. "Privacy-Preserving Collaborative Model Learning: The Case of Word Vector Training". *IEEE Transactions on Knowledge and Data Engineering (TKDE), 30(12): 2381-2393, 2018 (CCF-A).*
8. Yanjiao Chen, Xin Tian, Qian Wang, Minghui Li, **Minxin Du**, and Qi Li. "ARMOR: A Secure Combinatorial Auction for Heterogeneous Spectrum". *IEEE Transactions on Mobile Computing (TMC), 18(10): 2270-2284, 2018 (CCF-A).*
9. Qian Wang, Meiqi He, **Minxin Du**, Sherman S. M. Chow, Russell W. F. Lai, and Qin Zou. "Searchable Encryption over Feature-Rich Data". *IEEE Transactions on Dependable and Secure Computing (TDSC),15(3): 496-510, 2018 (CCF-A).*
10. Shengshan Hu, Minghui Li, Qian Wang, Sherman S. M. Chow, and **Minxin Du**. "Outsourced Biometric Identification with Privacy". *IEEE Transactions on information forensics and security (TIFS), 13(10): 2448-2463, 2018 (CCF-A).*

Teaching

- Spring 2025: EIE553 Security in Data Communication (52 MSc students)

Students

- **Xiaoyu Xu** (Ph.D.): working on machine unlearning (co-advised with Prof. Haibo Hu)
- **Youlong Ding** (RA): working on applied crypto

Services

PC member:
2025: ACM CCS, USENIX Security, PoPETs
2024: ACM CCS, USENIX Security, NeurIPS (Datasets and Benchmarks Track), IEEE ICDCS, AAAI
2023: AAAI

External Reviewer:
ACM CCS, USENIX Security, NDSS, IEEE S&P, CRYPTO, ASIACRYPT
INFOCOM, TheWeb, ESORICS, AsiaCCS, ACNS, PST *etc.*

Invited Journal Reviewer:
IEEE Transactions on Dependable and Secure Computing (TDSC)
IEEE Transactions on Information Forensics and Security (TIFS)
IEEE Transactions on Knowledge and Data Engineering (TKDE)
IEEE Transactions on Networking (ToN)
IEEE Transactions on Mobile Computing (TMC)
ACM Transactions on Privacy and Security (TOPS)
IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)
IEEE Transactions on Services Computing (TSC)
IEEE Transactions on Emerging Topics in Computing (TETC)
IEEE Internet of Things Journal (IoTJ)

Selected Talks

- "Differential Privacy for Text Analytics via Forward-Pass Signal Sanitization", at West Lake Forum, Zhejiang University, China, Jan. 2025.
- "DP-Forward: Fine-tuning and Inference on Language Models with Differential Privacy in Forward Pass", at Meta Central Applied Science PPML Group Seminar, Aug. 2024.
- "DP-Forward: Fine-tuning and Inference on Language Models with Differential Privacy in Forward Pass", at ACM CCS, Nov. 2023.
- "Sanitizing Sentence Embeddings (and Labels) for Local Differential Privacy", at ACM TheWebConf, May 2023.