Minxin Du

Department of Information Engineering
The Chinese University of Hong Kong
Shatin, NT, Hong Kong, China

Mobile: (+852) 5423 9412
Email: mxdu@ie.cuhk.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), Privacy-preserving Machine (Un)Learning, Secure Outsourcing or Multi-party Computation, Information Retrieval, *etc.*

Education and Working Experiences

The Chinese University of Hong Kong — Hong Kong, China
Research Associate/Post-doc (at Dept. of IE) — 11/2023-present
Host: Prof. Sherman S. M. Chow

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

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

Wuhan University — Wuhan, Hubei, China
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)
- 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)

Publications

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

1. **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". *ACM CCS '23.*
2. **Minxin Du**, Xiang Yue, Sherman S. M. Chow, Huan Sun. "Sanitizing Sentence Embeddings (and Labels) for Local Differential Privacy". *ACM TheWebConf '23.*
3. Yu Zheng, Wei Song, **Minxin Du**, Sherman Chow, Qian Lou, and Xiuhua Wang. "Cryptography-Inspired Federated Learning for Generative Adversarial Networks and Meta Learning". *ADMA'23.*

4. Yu Zheng, Heng Tian, **Minxin Du**[#], and Chong Fu. "Sanitizing Sentence Embeddings (and Labels) for Local Differential Privacy". *ACM MMSys '22 (Best Student Paper).*
5. Xiang Yue, **Minxin Du**[*], Tianhao Wang, Yaliang Li, Huan Sun, and Sherman S. M. Chow. "Differential Privacy for Text Analytics via Natural Text Sanitization". *Findings of ACL '21.*
6. Jiafan Wang, **Minxin Du**[*], and Sherman S. M. Chow. "Stargazing in the Dark: Secure Skyline Queries with SGX". *DASFAA '20.*
7. Minghui Li, Mingxue Zhang, Qian Wang, Sherman S. M. Chow, **Minxin Du**, Yanjiao Chen, and Chenliang Li. "InstantCryptoGram: Secure Image Retrieval Service". *INFOCOM '18.*
8. Qian Wang, Kui Ren, **Minxin Du**, Qi Li, and Aziz Mohaisen. "SecGDB: Graph Encryption for Exact Shortest Distance Queries with Efficient Updates". *FC '17 (Main Contributor).*
9. Qian Wang, Shengshan Hu, **Minxin Du**, Jingjun Wang, and Kui Ren. "Learning Privately: Privacy-Preserving Canonical Correlation Analysis for Cross-Media Retrieval". *INFOCOM '17.*
10. 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". *INFOCOM '16.*
11. Qian Wang, Shengshan Hu, Kui Ren, Meiqi He, **Minxin Du**, and Zhibo Wang. "CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud". *ESORICS'15.*

Refereed Journal Papers (in chronological order)

1. **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.*
2. **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, 2020.* (Extension of FC'17)
3. **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, Vol. 13, No. 11, pp. 2320-2332, 2018.*
4. 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, Vol. 30, No. 12, pp. 2381 - 2393, 2018.* (Main Contributor)
5. 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, Vol. 18, No. 10, pp. 2270-2284, 2019.*
6. 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, Vol. 15, No. 3, pp. 496 - 510, 2018.* (Main Contributor)
7. 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, Vol. 13, No. 10, pp. 2448 - 2463, 2018.*

Professional Experience

- PC Member for ACM CCS 2024, Usenix Security 2024, IEEE ICDCS 2024, AAAI 2022–24
- External Reviewer for Usenix Sec. 2021–24, ACM CCS 2022–23, NDSS 2022–24, AsiaCrypt 2023, CRYPTO 2019, TheWeb 2021–24, ICDCS 2020, 22–23, ESORICS 2019-20, ACNS 2020, 23–24 *etc.*
- Reviewer for IEEE Transactions on Dependable and Secure Computing (57 submissions)
- Reviewer for IEEE Transactions on Information Forensics and Security (4 submissions)
- Reviewer for IEEE Transactions on Knowledge and Data Engineering (2 submissions)