Minxin Du

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

Mobile: (+852) 5423 9412
Email: dm018@ie.cuhk.edu.hk
Website: duminxin.github.io

Research Interests Differential Privacy and Applied Cryptography (e.g., Searchable Encryption)

Education

The Chinese University of Hong Kong Hong Kong, China
Ph.D., Department of Information Engineering 08/2018-present
Advisor: Prof. Sherman S. M. 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

- Best Student Paper Award, ACM MMSys 2022
- Outstanding Teaching Assistant Award (2nd Term, 2020-2021)
- **Postgraduate Second-class Academic Innovation Award** (2019) (Bonus: 15,000 RMB)
- Student Stipend for Crypto Innovation School 2018 (Amount: 500 USD)
- Scholarship of Cyber Security, China Internet Development Foundation (Bonus: 50,000 RMB)
- **Postgraduate National Scholarship** (2017-2018) (Top 24 out of 344, bonus: 20,000 RMB)
- Postgraduate Second-class Scholarship (2017-2018) (Rank: top 30%, bonus: 2,000 RMB)
- 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)

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". *in submission.*

2. **Minxin Du**, Sherman S. M. Chow, Qian Wang, and Xiang Yue. "Private Genomic Diagnosis Retrieval with SGX". *in submission.*

3. **Minxin Du**, Xiang Yue, Sherman S. M. Chow, Huan Sun. "Sanitizing Sentence Embeddings (and Labels) for Local Differential Privacy". *ACM TheWebConf '23.*

4. 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-IJCNLP'21, online, (Co-first author).*

5. Jiafan Wang, **Minxin Du***, and Sherman S. M. Chow. "Stargazing in the Dark: Secure Skyline Queries with SGX". *DASFAA'20, Jeju, Korea, 2020 (Co-first author).*

6. Minghui Li, Mingxue Zhang, Qian Wang, Sherman S. M. Chow, **Minxin Du**, Yanjiao Chen, and Chenliang Li. "InstantCryptoGram: Secure Image Retrieval Service". *IEEE INFOCOM'18, Honolulu, HI, USA, April 15-19, 2018.*

7. Qian Wang, Kui Ren, **Minxin Du**, Qi Li, and Aziz Mohaisen. "SecGDB: Graph Encryption for Exact Shortest Distance Queries with Efficient Updates". *FC'17, Malta, April 3-7, 2017.* (Main Contributor)

8. Qian Wang, Shengshan Hu, **Minxin Du**, Jingjun Wang, and Kui Ren. "Learning Privately: Privacy-Preserving Canonical Correlation Analysis for Cross-Media Retrieval". *IEEE INFO-COM'17, Atlanta, GA, USA, May 1-4, 2017.*

9. 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". *IEEE INFOCOM'16, San Francisco, CA, USA, April 10-15, 2016.*

10. 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, Vienna, Austria, September 21-25, 2015.*

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 AAAI '23'22

- External Reviewer for Usenix Security '23'22'21, ACM CCS '23'22, NDSS '23'22, CRYPTO'19, TheWeb 23'22'21, ICDCS '22'20, ESORICS '20'19, ACNS '23'20 *etc.*

- Reviewer for IEEE Transactions on Dependable and Secure Computing

- Reviewer for IEEE Transactions on Information Forensics and Security

- Reviewer for IEEE Transactions on Knowledge and Data Engineering