Ye Dong (董业)

MinZhuang Road No. 89, Beijing, China
19950512dy@gmail.com

RESUME

I am Ye Dong (董业), a Ph.D. student at Institute of Information Engineering, Chinese Academy of Sciences (IIE, CAS) and School of Cyber Security, University of Chinese Academy of Sciences (UCAS), under Prof. *Xiaojun Chen*. I got my bachelor degree in School of Computer Science and Technology, Shandong University (SDU), and had been an exchange student in School of Computer, Beijing Institute of Technology (BIT). I had been one Research Assistant at NETWORK & INFORMATION SECURITY LAB (ISec) under Prof. *Qiuliang Xu*.

RESEARCH TOPICS

Privacy-Preserving Enhancement Technologies, **Secure Multi-Party Computation**, **Homomorphic Encryption**, **Distributed Machine Learning**, and **Federated Learning**.

EDUCATION

Ph.D. Student in Cyber Security
IIE, CAS & School of Cyber Security, UCAS Sep. 2018-Now.

B.S. Degree in Computer Science and Technology
School of Computer Science and Technology, SDU Sep. 2014-June 2018

- **Exchange Student**
  School of Computer, BIT Sep. 2015-June 2016
- **Research Assistant**
  ISec LAB, SDU Oct. 2016-June 2018

WORK

Research Assistant
ISec LAB, SDU Oct. 2016-June 2018

Teaching Assistant
Big Data Security and Privacy Preserving, UCAS Summer, 2021

PUBLICATION

1. Yiran Liu, **Ye Dong**, Hao Wang, Han Jiang, Qiuliang Xu. Distributed Fog Computing and Federated Learning enabled Secure Aggregation for IoT Devices. IEEE IoT'22. [pdf].
2. Zhendong Zhao, Xiaojun Chen, Yuexin Xuan, **Ye Dong**, Dakui Wang, Kaitai Liang. DEFEAT: Deep Hidden Feature Backdoor Attacks by Imperceptible Perturbation and Latent Representation Constraints. CVPR'22. [pdf].
3. Kaiyun Li, Xiaojun Chen, **Ye Dong**, Peng Zhang, Dakui Wang, Shuai Zeng. Efficient Byzantine-Resilient Stochastic Gradient Descent. FTL-IJCAI'21. [pdf].

4. **Ye Dong**, Xiaojun Chen, Kaiyun Li, Dakui Wang, Shuai Zeng. FLOD: Oblivious Defender for Private Byzantine-Robust Federated Learning with Dishonest-Majority. ESORICS'21. [pdf].
5. **Ye Dong**, Xiaojun Chen, Liyan Shen, Dakui Wang. EaSTFLy: Efficient and secure ternary federated learning. Computer & Security'20. [pdf].
6. **Ye Dong**, Wei Hou, Xiaojun Chen, Shuai Zeng. Efficient and Secure Federated Learning Based on Secret Sharing and Gradients Selection. Journal of Computer Research and Development'20. (In Chinese). [pdf].
7. Liyan Shen, Xiaojun Chen, Jinqiao Shi, **Ye Dong**, Binxing Fang. An Efficient 3-Party Framework for Privacy-Preserving Neural Network Inference. ESORICS'20. [pdf].
8. **Ye Dong**, Xiaojun Chen, Liyan Shen, Dakui Wang. Privacy-Preserving Distributed Machine Learning Based on Secret Sharing. ICICS'19. [pdf].
9. Liyan Shen, Xiaojun Chen, Dakui Wang, Binxing Fang, **Ye Dong**. Efficient and Private Set Intersection of Human Genomes. BIBM'18. [pdf].

RESEARCH MATERIALS

- Paper list of Privacy-Preserving Machine Learning. [Link]
- Blogs for Privacy-Preserving Machine Learning. (In Chinese). [Link]

TECHNICAL STRENGTHS

Program Languages: Python, C/C++, MATLAB.
Software & Tools: PyTorch, LATEX, Adobe Illustrator.

HONORS & AWARDS

- Merit Student, from UCAS. (2020 & 2021).
- Institute Excellence Award, from IIE, CAS. (2020).
- Second Campus Scholarship, from SDU. (2016).
- School Scholarships, from BIT. (2016).
- School Scholarships, from SDU. (Multiple Times).

MISCELLANY

- Presentation for 26th European Symposium on Research in Computer Security (ESORICS'21), Virtual, Oct., 2021.
- Reviewer for IEEE Systems Journal.
- Attend CCF-YEF2021, Shenyang, May, 2021.
- Attend the 25th European Symposium on Research in Computer Security (ESORICS'20), co-author, Virtual, Sep., 2020.
- Subreviewer for the 2020 International Conference on Frontiers in Cyber Security (FCS'20).
- Presentation for the 21st International Conference on Information and Communications Security (ICICS'19), Beijing, Dec, 2019.