Ye Dong

Curriculum Vitae

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

Personal Data

Email `19950512dy@gmail.com`.

Citizenship **Shandong, China**.

Web `https://ye-d.github.io/`.

Research Topics

Secure Multiparty Computation

Familiar **Secret Sharing, Oblivious Transfer, Garbled Circuits**.

Basic **Homomorphic Encryption**.

Security and Privacy of Machine (Deep) Learning

Familiar **MPC-Private ML/DL, Secure Aggregation of Federated Learning**.

Basic **Byzantine-Robustness, Attacks & Privacy Leakages, Quantization Technologies**.

Education

Sep. 2018 – Present **PhD in Cyber Security, (expect to graduate in May. 2023)**, *Institute of Information Engineering, Chinese Academy of Sciences & School of Cyber Security, University of Chinese Academy of Sciences*, Beijing, China.

Sep. 2014 – June. 2018 **Bachelor in Computer Science and Technology**, *Shandong University*, Jinan, Shandong.

Sep. 2015 – June. 2016 **Exchange Student**, *School of Computer, Beijing Institute of Technology*, Beijing, China.

Theses

PhD Thesis (Institute of Information Engineering, CAS; Ongoing)

Title *Research on Key Technologies of Practical Secure Multi-Party Computation in Deep Learning*

Supervisors Xiaojuen Chen

Bachelor Thesis (Shandong University; June. 2018)

Title *Privacy-Preservation and Mining of Zcash*

Supervisor Han Jiang

Previous Experience

Teaching & Work

Summer. 2021 & 2022 **Teaching Assistant**, *University of CAS*, Beijing, China.
Big Data Security and Privacy-Preserving

Mar. 2022 – Sep. 2022 **External Consulting**, *Primihub*, Beijing, China.
Consultancy services on Multi-Party Computation and related technologies

Oct. 2016 – June. 2018 **Research Assistant**, *Network and Information Security Lab, Shandong University*, Jinan, China.

Supervisor Prof. Qiulaing Xu & Prof. Han Jiang

Community Service

Dec. 2022 **Reviewer**, *CVPR*.
Reviewer for the IEEE / CVF Computer Vision and Pattern Recognition Conference 2023

Sep. 2022 **Reviewer**, *CASE*.
Reviewer for the 7th International Conference on Computer Science and Application Engineering 2022

Sep. 2021 **Reviewer**, *IEEE Systems Journal*.
Reviewer for the IEEE Systems Journal 2021

Jul. 2020 **External Reviewer**, *FCS*.
External Reviewer for the International Conference on Frontiers in Cyber Security 2020

Others

Jul. 2022 **Attendance**, *DAC*, Hybrid Conference, Co-author.
Attend the 59th Design Automation Conference

May. 2021 **Attendance**, *CCF-YEF*, Shenyang, China.

Sep. 2020 **Attendance**, *ESORICS*, Online Conference, Co-author.
Attend the 25th European Symposium on Research in Computer Security

Languages

Chinese Native

English Fluent

Computer Skills

OS	Linux, Windows, MacOX	Typography	LaTeX, Microsoft Office, Markdown
Scientific	Octave, Pytorch, Tensorflow	Programming	Python, C, C++, Shell

Open-Source Projects

CryptoFL **CryptoFL: Cryptographically Secure Aggregation for Federated Learning**.
`https://github.com/Ye-D/CryptoFL`

METEOR **Meteor: Improved Secure 3-Party Neural Network Inference with Reducing Online Communication Costs**.
`https://github.com/Ye-D/Meteor`

Awesome Lists

PPML-Resource **Privacy-Preserving-Machine-Learning-Resources** .
`https://github.com/Ye-D/PPML-Resource`

APC **Awesome Privacy Computing** .
`https://github.com/primihub/Awesome-Privacy-Computing`

Awards

2020 & 2021 **Merit Student Award**, *University of CAS*.

2020 **Institute Excellence Award**, *Institute of Information Engineering, CAS*.

2016 **Exchange Campus Scholarship**, *Shandong University*.

2015 **School Scholarship**, *Beijing Institute of Technology*.

2014 – 2018 **School Scholarships**, *Shandong University*, Multiple Times.

Talks

Oct. 2021 **FLOD: Oblivious Defender for Private Byzantine-Robust Federated Learning with Dishonest-Majority**, *ESORICS 2021*, Virtual Conference.

Dec. 2019 **Privacy-Preserving Distributed Machine Learning Based on Secret Sharing**, *ICICS 2019*, Beijing, China.

Publications

1. Ye Dong, Xiaojun Chen, Weizhan Jing, Kaiyun Li, and Weiping Wang. METEOR: Improved secure 3-party neural network inference with reducing online communication costs. *Cryptology ePrint Archive,* ***Accepted to WWW'2023, CORE Rank A****, 2023.

2. Liyan Shen, Ye Dong, Binxing Fang, Jinqiao Shi, Xuebin Wang, Shengli Pan, and Ruisheng Shi. Abnn^2: secure two-party arbitrary-bitwidth quantized neural network predictions. In ***Proceedings of the 59th ACM/IEEE Design Automation Conference, CORE Rank A***, pages 361–366, 2022.

3. Yiran Liu, Ye Dong, Hao Wang, Han Jiang, and Qiuliang Xu. Distributed fog computing and federated learning enabled secure aggregation for iot devices. *IEEE Internet of Things Journal*, 2022.

4. Zhendong Zhao, Xiaojun Chen, Yuexin Xuan, Ye Dong, Dakui Wang, and Kaitai Liang. Defeat: Deep hidden feature backdoor attacks by imperceptible perturbation and latent representation constraints. In ***Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, CORE Rank A****, pages 15213–15222, 2022.

5. Ye Dong, Xiaojun Chen, Kaiyun Li, Dakui Wang, and Shuai Zeng. Flod: Oblivious defender for private byzantine-robust federated learning with dishonest-majority. In ***European Symposium on Research in Computer Security, CORE Rank A***, pages 497–518. Springer, 2021.

6. Kaiyun Li, Xiaojun Chen, Ye Dong, Peng Zhang, Dakui Wang, and Shuai Zen. Efficient byzantine-resilient stochastic gradient descent. *FL-Workshop@IJCAI*, 2021.

7. Dong Ye, Hou Wei, Chen Xiaojun, and Zeng Shuai. Efficient and secure federated learning based on secret sharing and gradients selection. *Journal of Computer Research and Development*, 57(10):2241, 2020.

8. Liyan Shen, Xiaojun Chen, Jinqiao Shi, Ye Dong, and Binxing Fang. An efficient 3-party framework for privacy-preserving neural network inference. In ***European Symposium on Research in Computer Security, CORE Rank A***, pages 419–439. Springer, 2020.

9. Ye Dong, Xiaojun Chen, Liyan Shen, and Dakui Wang. Eastfly: Efficient and secure ternary federated learning. *Computers & Security, CORE Rank B*, 94:101824, 2020.

10. Ye Dong, Xiaojun Chen, Liyan Shen, and Dakui Wang. Privacy-preserving distributed machine learning based on secret sharing. In *Information and Communications Security: 21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers 21, CORE Rank B*, pages 684–702. Springer, 2020.

11. Liyan Shen, Xiaojun Chen, Dakui Wang, Binxing Fang, and Ye Dong. Efficient and private set intersection of human genomes. In *2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), short paper*, pages 761–764. IEEE, 2018.