Ye Dong

Curriculum Vitae

National University of Singapore
✉ *dongye@nus.edu.sg*
Webpage
Github *Linkedin*

I am serving as a Research Fellow at the National University of Singapore, co-supervised by *Prof. Jin-Song Dong* and *Prof. Tianwei Zhang* from Nanyang Technological University. I got Ph.D. degree in Cyberspace Security with *Outstanding Graduation Award* from the Institute of Information Engineering, Chinese Academy of Sciences, and bachelor degree from the School of Computer Science and Technology, Shandong University.

Education

Sep. 2018 – June. 2023 **Ph.D. in Cyberspace Security**, *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**, *School of Computer Science and Technology, Shandong University*, Jinan, Shandong, China.

Theses

Ph.D. Thesis (Institute of Information Engineering, CAS; June. 2023)

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

Supervisors Prof. Xiaojuen Chen

Bachelor Thesis (Shandong University; June. 2018)

Title *Privacy-Preservation and Mining of ZCash*

Supervisor Prof. Han Jiang

Research Experience

Jan. 2025 – *Present* **Research Fellow**, *School of Computing, National University of Singapore*.
Secure Private, & Verifiable AI, Supervised by *Prof. Jin-Song Dong* and *Prof. Tianwei Zhang*@NTU.

Jan. 2024 – *Jan. 2025* **Research Fellow**, *iTrust, Singapore University of Technology and Design*.
IoT Security, Supervised by *Prof. Jianying Zhou* and *Prof. Sudipta Chattopadhyay*.

Sep. 2023 – Oct. 2023 **Research Assistant**, *Institute for Artificial Intelligence and the School of Integrated Circuits, Peking University*, Beijing, China.
Secure Inference of Large Language Models, Supervised by *Prof. Meng Li*.

Apr. 2023 – July. 2023 **Research Intern**, *Ant Cryptograhpy & Privacy Lab, Ant Group*, Beijing, China.
Practical Cryptographic Techniques, Supervised by *Dr. Cheng Hong*.

Mar. 2022 – Sep. 2022 **Research Intern**, *PRIMITIVE HUB*, Beijing, China.
Consultancy services on Multi-Party Computation and related technologies

Oct. 2016 – June. 2018 **Research Assistant**, *Cryptography and Privacy Computing Laboratory, Shandong University*, Jinan, China.
Cryptographic Techniques for Cryptocurrency, Supervised by *Prof. Qiuliang Xu* & *Prof. Han Jiang*

Mentorship

Jul. 2-25 – Sep. 2025 **Thomas Fargues**, *Research Intern@NTU*, Co-Advised with: Tianwei Zhang@NTU.
Topic: Private Large Language Model, Watermarking, Safety. Result: [under peer-review]

Sep. 2023 – Jan. 2025 **Wenxuan Zeng**, *Ph.D@PKU*, Co-Advised with: Meng Li@PKU.
Topic: Private Large Language Model, System Security. Result: [NeurIPS 2025]

Jun. 2023 – Jan. 2025 **Ruonan Chen**, *Ph.D@BUAA*, Co-Advised with: Jianwei Liu@BUAA and Jianying Zhou@SUTD.
Topic: Blockchain, Federated Learning, Secure Aggregation. Result: [WWW 2025]

Jan. 2024 – Dec. 2024 **Yansong Zhang**, *Ph.D@IIE,CAS*, Co-Advised with: Xiaojun Chen@IIE,CAS.
Topic: Secure Neural Networks, Malicious Security MPC. Result: [IEEE TIFS 2025]

Oct. 2022 – June. 2024 **Tingyu Fan**, *Ph.D@IIE,CAS*, Co-Advised with: Xiaojun Chen@IIE,CAS.
Topic: GPU-accelerated Secure Neural Networks, Federated Learning. Result: [ICC 2024, ACSAC 2024]

Oct. 2022 – June. 2023 **Weizhan Jing**, *Ph.D@IIE,CAS*, Co-Advised with: Xiaojun Chen@IIE,CAS.
Topic: Private Set Intersection. Result: [TrustCom 2025]

Professional Services

Chair **ACNSW-SiMLA'2025**.

Program Committee **Eurosys'2026 (Shadow), CCS'2025 (Poster/Demo), EAI-MobiQuitous'2025, CCSW-WPES'2025, RAID'2025, PoPETs'2025&2026**.

Conf. Reviewer **ACNS‘2026 (external), CVPR'2026&2022, NeurIPS'2025 (Position Paper Track), AVSS'2025, KDD'2025, CODASPY'2025 (sub), WWW'2025, ICME'2024-26, FCS'2020**.

Journal. Reviewer **TDSC, TIFS, TSC, TWEB, ACM Computing Surveys, IACR CiC (Editorial Board Member) 2025&2026, Scientific Reports, Information Sciences, Information Fusion, IEEE Systems Journal, Cybersecurity, Computer Networks, Computer Standards & Interfaces**.

Presentations & Invited Talks

Dec. 2025 **MIZAR: Boosting Secure Three-party Deep Learning with Co-Designed Sign-Bit Extraction and GPU Acceleration**, *ACSAC 2025*, Honolulu, Hawaii, USA.

Sep. 2025 **MIZAR: Boosting Secure Three-party Deep Learning with Co-Designed Sign-Bit Extraction and GPU Acceleration**, *NTU CYSREN and Sweden WASP Joint Workshop 2025*, Nanyang Technological University, Singapore.

May. 2023 **METEOR: Improved Secure 3-Party Neural Network Inference with Reducing Online Communication Costs**, *WWW 2023*, Austin, USA.

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.

Awards

2023 **Outstanding Ph.D. Graduate Award**, *IIE, CAS*.

2023 **CAS Presidential Scholarship (Excellent Prize)**, *CAS*.

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.

Open-Source Projects

CPS4AI **Cryptography, Privacy, and Security for Artificial Intelligence**.
`https://github.com/CPS4AI`

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

Publications

Citations:689; h-index: 13; i10-index:13, ✉ *denotes the corresponding author.*

Conference

2026 **Ye Dong**✉, Yan Lin Aung, Sudipta Chattopadhyay, and Jianying Zhou. ChatIoT: Large language model-based security assistant for internet of things with RAG. In *24th International Conference on Applied Cryptography and Network Security (ACNS), To appear*, 2026. **AR:20.9% (Cycle 1)**. **Citation:9**.

2026 Xiangfu Song, Jianli Bai, **Ye Dong**✉, Yijian Liu, Yu Zhang, Xianhui Lu, and Tianwei Zhang. Streaming Function Secret Sharing and Its Applications. In *35th USENIX Security Symposium (USENIX Security), To appear*, 2026. **AR:14%**. **Citation:0**.

2025 Wenxuan Zeng, **Ye Dong**, Jinjin Zhou, Junming Ma, Jin Tan, Runsheng Wang, and Meng Li✉. MPCache: MPC-friendly KV Cache eviction for efficient private large language model inference. In *39th Annual Conference on Neural Information Processing Systems (NeurIPS)*, 2025. **AR:24.52%**. **Citation:5**.

2025 Yaxi Yang, Xiaojian Liang, Xiangfu Song✉, **Ye Dong**, Linting Huang, Hongyu Ren, Changyu Dong✉, and Jianying Zhou. Maliciously secure circuit private set intersection via SPDZ-compatible oblivious PRF. In *25th Privacy Enhancing Technologies Symposium (PETS)*, 2025. **AR:26%**. **Citation:2**.

2025 Yuexin Xuan, Xiaojun Chen✉, Zhendong Zhao, **Ye Dong**, Xin Zhao, and Bisheng Tang. Practical and general backdoor attacks against personalized federated learning. In *32nd International Conference on Neural Information Processing (ICONIP)*, 2025. **AR:39%**. **Citation:0**.

2025 Cheng Wang, Yan Lin Aung✉, **Ye Dong**, Trupil Limbasiya, and Jianying Zhou. LAPIS: Layered anomaly detection system for IoT Security. In *7th International Workshop on Artificial Intelligence and IoT Security In Conjunction with the 23rd International Conference on Applied Cryptography and Network Security (AIoTS@ACNS)*, 2025. **AR:N/A**. **Citation:0**.

2025 **Ye Dong**, Xudong Chen, Xiangfu Song, Yaxi Yang✉, Tianwei Zhang, and Jin-Song Dong. MIZAR: Boosting secure three-party deep learning with co-designed sign-bit extraction and GPU acceleration. In *41st Annual Computer Security Applications Conference (ACSAC)*, 2025. **AR:18.8%**. **Citation:1**.

2025 Weizhan Jing, Xiaojun Chen✉, Xudong Chen, **Ye Dong**, Yaxi Yang, and Qiang Liu. VCR: Fast private set intersection with improved VOLE and CRT-batching. In *24th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2025. **AR:N/A**. **Citation:0**.

2025 Ruonan Chen, **Ye Dong**, Yizhong Liu, Tingyu Fan, Dawei Li, Zhenyu Guan, Jianwei Liu✉, and Jianying Zhou. FLock: Robust and privacy-preserving federated learning based on practical blockchain state channels. In *34th ACM Web Conference (WWW)*, 2025. **AR:19.8%**. **Citation:5**.

2024 Qifan Wang, Shujie Cui, Lei Zhou✉, **Ye Dong**, Jianli Bai, Yun Sing Koh, and Giovanni Russello. GTree: Gpu-friendly privacy-preserving decision tree training and inference. In *23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2024. **AR:19.8%**. **Citation:2**.

2024 Qiang Liu, Xiaojun Chen✉, Weizhan Jing, and **Ye Dong**. An effective multiple private set intersection. In *20th EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2024. **AR:36%**. **Citation:1**.

2024 Tingyu Fan, Xiaojun Chen✉, **Ye Dong**, Xudong Chen, and Weizhan Jing. Lightweight secure aggregation for personalized federated learning with backdoor resistance. In *40th Annual Computer Security Applications Conference (ACSAC)*, 2024. **AR:21.8%**. **Citation:1**.

2024 Tingyu Fan, Xiaojun Chen✉, **Ye Dong**, Xudong Chen, and Weizhan Jing. Comet: Communication-efficient batch secure three-party neural network inference with client-aiding. In *IEEE International Conference on Communications (ICC)*, 2024. **AR:39.7%**. **Citation:1**.

2024 Xudong Chen, Xiaojun Chen✉, **Ye Dong**, Weizhan Jing, Tingyu Fan, and Qiang Liu. Roger: A round optimized gpu-friendly secure inference framework. In *IEEE International Conference on Communications (ICC)*, 2024. **AR:39.7%**. **Citation:2**.

2023 Yuexin Xuan, Xiaojun Chen✉, Zhendong Zhao, Bisheng Tang, and **Ye Dong**. Practical and general backdoor attacks against vertical federated learning. In *16th European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD)*, 2023. **AR:24%**. **Citation:15**.

2023 **Ye Dong**, Xiaojun Chen✉, Weizhan Jing, Li Kaiyun, and Weiping Wang. Meteor: Improved secure 3-party neural network inference with reducing online communication costs. In *32rd ACM Web Conference (WWW)*, 2023. **AR:19.2%**. **Citation:32**.

2022 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 *35th IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2022. **AR:25.3%**. **Citation:117**.

2022 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 *59th ACM/IEEE Design Automation Conference (DAC)*, 2022. **AR:22.7%**. **Citation:22**.

2021 **Ye Dong**, Xiaojun Chen✉, Kaiyun Li, Dakui Wang, and Shuai Zeng. FLOD: Oblivious defender for private byzantine-robust federated learning with dishonest-majority. In *26th European Symposium on Research in Computer Security (ESORICS)*, 2021. **AR:20.2%**. **Citation:104**.

2021 Kaiyun Li, Xiaojun Chen✉, **Ye Dong**, Peng Zhang, Dakui Wang, and Shuai Zen. Efficient byzantine-resilient stochastic gradient descent. In *International Workshop on Federated and Transfer Learning for Data Sparsity and Confidentiality in Conjunction with IJCAI (FTL-Workshop@IJCAI)*, 2021. **AR:N/A**. **Citation:0**.

2020 Liyan Shen✉, Xiaojun Chen, Jinqiao Shi, **Ye Dong**, and Binxing Fang. An efficient 3-party framework for privacy-preserving neural network inference. In *25th European Symposium on Research in Computer Security (ESORICS)*, 2020. **AR:19.7%**. **Citation:18**.

2019 **Ye Dong**, Xiaojun Chen✉, Liyan Shen, and Dakui Wang. Privacy-preserving distributed machine learning based on secret sharing. In *21st International Conference on Information and Communications Security (ICICS)*, 2019. **AR:23.6%**. **Citation:36**.

2018 Liyan Shen, Xiaojun Chen, Dakui Wang, Binxing Fang, and **Ye Dong**. Efficient and private set intersection of human genomes. In *19th IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 2018. **AR:19.3%**. **Citation:34**.

Journal/Transactions

2025 Yansong Zhang, Xiaojun Chen✉, **Ye Dong**, Qinghui Zhang, Rui Hou, Qiang Liu, and Xudong Chen. MD-SONIC: Maliciously-secure outsourcing neural network inference with reduced online communication. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2025, **Impact Factor:8.0**, **Citation:3**.

2025 Qifan Wang, Shujie Cui✉, Lei Zhou, **Ye Dong**, Jianli Bai, Yun Sing Koh, and Giovanni Russello. XGT: Fast and secure decision tree training and inference on GPUs. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2025, **Impact Factor:7.5**, **Citation:0**.

2025 **Ye Dong**, Wenjie Lu✉, Xiaoyang Hou, Kang Yang, and Jian Liu. M&M: Secure Two-Party Machine Learning through Efficient Modulus Conversion and Mixed-Mode Protocols. *Transactions on Dependable and Secure Computing (TDSC)*, 2025, **Impact Factor:7.5**, **Citation:0**.

2025 **Ye Dong**, Wenjie Lu, Yancheng Zheng, Haoqi Wu, Derun Zhao, Jin Tan, Zhicong Huang, Cheng Hong✉, Tao Wei, Wenguang Chen, and Jianying Zhou. PUMA: Secure inference of llama-7b in five minutes. *Security & Safety*, 2025, **Impact Factor:N/A**, **Citation:104**.

2025 **Ye Dong**, Xudong Chen, Xiangfu Song✉, Yaxi Yang, Wen jie Lu, Tianwei Zhang, Jianying Zhou, and Jin-Song Dong. Alkaid: Accelerating Three-Party Boolean Circuits by Mixing Correlations and Redundancy. *Transactions on Information Forensics & Security (TIFS)*, 2025, **Impact Factor:8.0**, **Citation:0**.

2025 Jinglong Luo, Zhuo Zhang Yehong Zhang, Shiyu Liu, **Ye Dong**, Haoran Li, Yue Yu, Hui Wang, Xun Zhou✉, and Zenglin Xu. Cryptography-based privacy-preserving large language models: a lifecycle survey of frameworks, methods, and future directions. *Artificial Intelligence Review*, 2025, **Impact Factor:13.9**, **Citation:0**.

2025 Tingyu Fan, Xiaojun Chen✉, Xudong Chen, **Ye Dong**, Weizhan Jing, and Zhendong Zhao. Fedshelter: Efficient privacy-preserving federated learning with poisoning resistance for resource-constrained iot network. *Computer Networks*, 2025, **Impact Factor:4.6**, **Citation:4**.

2024 Min Ma, Yu Fu✉, **Ye Dong**, Ximeng Liu, and Kai Huang. PODI: A private object detection inference framework for autonomous vehicles. *Knowledge-Based Systems, Elsevier*, 2024, **Impact Factor:8.0**, **Citation:5**.

2023 **Ye Dong**, Xiaojun Chen✉, Xiangfu Song, and Kaiyun Li. FlexBNN: Fast private binary neural network inference with flexible bit-width. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2023, **Impact Factor:8.0**, **Citation:13**.

2022 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, **Impact Factor:8.9**, **Citation:31**.

2020 **Ye Dong**, Wei Hou, Xiaojun Chen✉, and Shuai Zeng. Efficient and secure federated learning based on secret sharing and gradients selection. *Journal of Computer Research and Development (in Chinese)*, 2020, **Impact Factor:2.55**, **Citation:24**.

2020 **Ye Dong**, Xiaojun Chen✉, Liyan Shen, and Dakui Wang. EaSTFLy: Efficient and secure ternary federated learning. *Computers & Security, Elsevier*, 2020, **Impact Factor:5.4**, **Citation:123**.

Patents

2024 Ye Dong, Yan Lin Aung, Jianying Zhou, and Sudipta Chattopadhyay. ChatIoT: Large Language Model-Enabled Internet of Things Security Assistant. *Singapore Patent Application No. 10202402752Q, filed on 4 September*, 2024.