Bingzhe Wu

Room 512, science#5 building, Peking University, Beijing,100871

+8618628101267 • wubingzheagent@gmail.com
https://sites.google.com/view/bingzhe/home

I am currently a fourth-year Ph.D's student at Peking University. My research interests lie in secure machine learning, efficient deep learning and medical image analysis. I pay particular attention on secure machine learning. My previous research on secure machine learning focus on privacy analysis of different deep learning algorithms, developing privacy-preserving training/inference algorithms under data-isolated setting, and building theoretical framework for explainable secure machine learning.

Education

- **Peking University** — **Beijing**
  Computer Science, Ph.D — *2016–Now*

  Research Interests: Medical Image Analysis, Adversarial Generative Network, Object Detection
- **Peking University** — **Beijing**
  Mathematical Science, Bachelor — *2012–2016*

  Major: Engineering Computing

Award

- **2020: Apple Ph.D Fellowship** (Only one place in the China mainland.)
- **2020: The Ten Most Talented Researchers in EECS of Peking University**
- **2018: China National Scholarship**
- **2016:** Meritorious Winner of American Mathematical Contest In Modeling
- **2011:** The first-prize winner of China Middle School Mathematical Competition

Industrial Experience

- **Apple Research** — **London, UK**
  Research Intern, Secure Machine Learning — *Aug 2020–TBD*

  Privacy-preserving machine learning for the Siri system.
- **Ant Financial Services Group** — **Beijing, China**
  Research Intern, Secure Machine Learning — *April 2019–April 2020*

  I studied on using various cryptography protocols and Bayesian learning to build privacy-preserving deep learning algorithms for a number of analysis tasks on financial data.
- **IBM CRL** — **Beijing, China**
  Research Intern, Deep Learning Application in Medical Image Analysis — *Sep 2017–Sep2018*

  I studied on applying deep learning algorithms for various pathological and endoscopy image analysis tasks.
- **Google Machine Learning Summer Camp** — **Jeju, Korea**
  Participate, Topic: Single Image Super Resolution — *April 2017–Sep 2017*

  I developed a general framework for single image super resolution based on GAN and proposed a robust perceptual loss based on the framework
- **Otureo Inc** — **Beijing, China**
  Software Engineer — *August 2016 – Now*

I focus on developing and designing compact DNN models for face related tasks on embedded devices.

Service

- **Journal Reviewer:** TECS
- **Conference Reviewer:** ICLR, NeurIPS, AAAI

Technical and Personal Skill

- **Programming Language:** Proficient in:Python,
  Also basic ability with: C and C++.
- **Deep Learning Framework** Tensorflow, Pytorch, MXNet, Caffe.
- **Other:** Docker, LaTeX

Publication

Bingzhe Wu, Chaochao Chen, Shiwan Zhao, Cen Chen, Yuan Yao, Guangyu Sun, Li Wang, Xiaolu Zhang, and Jun Zhou. Characterizing membership privacy in stochastic gradient langevin dynamics. In *AAAI*, 2020.

Zhihang Yuan(*), **Bingzhe Wu(*)**, Zheng Liang, Shiwan Zhao, Weichen Bi, and Guangyu Sun. S2dnas: Transforming static cnn model for dynamic inference via neural architecture search. In *ECCV*, 2020 (* denotes equal contribution).

Bingzhe Wu, Shiwan Zhao, Haoyang Xu, ChaoChao Chen, Li Wang, Xiaolu Zhang, Guangyu Sun, and Jun Zhou. Generalization in generative adversarial networks: A novel perspective from privacy protection. In *NeurIPS*, 2019.

Peicheng Xie(*), **Bingzhe Wu(*)**, and Guangyu Sun. Bayhenn: Combining bayesian deep learning and homomorphic encryption for secure dnn inference. In *IJCAI*, 2019, (* denotes equal contribution).

Bingzhe Wu, Shiwan Zhao, Xiaolu Zhang, Zhong Su, Caihong Zeng, Zhihong Liu, and Guangyu Sun. P3sgd: Patient privacy preserving sgd for regularizing deep cnns in pathological image classification. In *CVPR*, 2019.

Bingzhe Wu, Xiaolu Zhang, Shiwan Zhao, Lingxi Xie, Caihong Zeng, Zhihong Liu, and Guangyu Sun. G2C: A Generator-to-Classifier Framework Integrating Multi-stained Visual Cues for Pathological Glomerulus Classification. In *AAAI*, 2019.

Bingzhe Wu, Zhichao Liu, Zhihang Yuan, Guangyu Sun, and Charles Wu. Reducing Overfitting in Deep Convolutional Neural Networks Using Redundancy Regularizer. In *International Conference on Artificial Neural Networks*, pages 49–55. Springer, 2017.

Chaochao Chen, Liang Li, **Bingzhe Wu**, Cheng Hong, Li Wang, and Jun Zhou. Secure social recommendation based on secret sharing. In *ECAI*, 2020.

Zhou Zhe(*), **Bingzhe Wu (*)**, Liang Zheng, Sun Guangyu, Xu Chenren, and Luo Guojie. Saface: Towards scenario-aware face recognition via edge computing system. In *HotEdege*, 2020 (* denotes equal contribution).

Preprints

Bingzhe Wu, Haodong Duan, Zhichao Liu, et al. SRPGAN: perceptual generative adversarial network for single image super resolution[J]. arXiv preprint arXiv:1712.05927, 2017.