

# QIAOYUE TANG

(+1)778-317-5073 | cathy.tangqiaoyue@gmail.com | qiaoyuet@cs.ubc.ca

---

## EDUCATION

### University of British Columbia

*Ph.D. in Computer Science, under supervision of Mathias Lécuyer*  
*Expected graduation: Late 2026 - Early 2027*

Vancouver, BC

*September 2021 – Now*

### University of British Columbia

*MSc. in Statistics, GPA: 91/100, under supervision of Lang Wu & Aline Talhouk*

Vancouver, BC

*September 2017 – July 2019*

### University of British Columbia

*BSc. in Statistics, Minor in Economics, GPA: 86/100*

Vancouver, BC

*September 2013 – June 2017*

---

## EXPERIENCE

### Machine Learning Research Intern

*Royal Bank of Canada, Borealis*

May 2025 – October 2025

*Vancouver, Canada*

### Machine Learning Engineer

*Huawei Technologies, AI Application Research Center*

August 2019 – August 2021

*Shenzhen, China*

### Graduate Research Assistant

*BC Cancer Research Center, OVCARE*

May 2018 – June 2019

*Vancouver, BC*

### Undergraduate Research Assistant

*Vancouver General Hospital, Eye Care Center*

September 2016 – January 2017

*Vancouver, BC*

---

## RESEARCH

My research focuses on data privacy, including (1) designing efficient privacy-preserving algorithms with provable guarantees, (2) auditing privacy leakage in trained machine learning models, and (3) adapting existing tools to domain-specific problems. I have also worked on broader responsible AI topics, such as (4) mitigating social bias and developing fairer models.

---

## SELECTED PROJECTS

### Private and Stable Test-time Adaptation

*Project at UBC*

- Incorporate differentially private training techniques to improve test-time adaptation (TTA) performances, where trained models adapt parameters in reducing error on new and distributionally different test data.
- Perform experiment and analysis for private TTA algorithms on pretrained ViT models and large-scale corrupted dataset ImageNet-C. [1]

### Improving model fairness on vision and language downstream tasks

*Project at RBC Borealis*

- Propose a coherent framework that improves both prediction- and representation-level fairness when fine-tuning downstream tasks from pre-trained models with potential social biases.
- Apply the proposed framework to both vision and language datasets and pre-trained models and show improved fairness performance while maintaining downstream prediction accuracy. [2]

### Privacy Auditing of Machine Learning Models without Retraining

*Project at UBC*

- Propose a framework using synthetic non-member data for evaluating membership inference attacks on the target model to audit its privacy level in practice.
- Perform theoretical analysis to provide rigorous guidelines for privacy auditing under the proposed framework. [4]
- Extending the framework in auditing large multi-model foundation models such as CLIP.

### Correcting DP Bias in Adam's Second Moment Estimation

*Project at UBC*

- Analyze the interaction between DP and the Adam optimizer, and show that DP noise introduces bias in Adam’s second moment estimator which reduce DP-Adam to DP-SGD with momentum and violates the sign-descent hypothesis for Adam’s performance.
- Propose a variation of DP-Adam that corrects for the bias introduced by DP noise, and analyze its theoretical properties.
- Evaluate the proposed method which yields significant improvements (up to 3.5 percentage points of test accuracy) over DP-Adam. [5]
- Extend to investigate under heavy-tail class imbalance with applications to language model fine-tuning. [3]

## Bug File Localization for Software Defect Tracking Systems

*Project at Huawei*

- Use historical data in closed issue documents to train a Sequence-to-Sequence model to capture implicit correspondence between user-submitted problem descriptions and the modified code file paths.
- Enhance model performance by incorporating source-code comment embedding and hard-coded rules on matching relevant files.
- Develop a utility tool based on the model to locate potential bug files in deep source-code directories to aid maintenance efficiency.
- Obtain > 55% hit-1 accuracy when recommending top-20 file paths when testing model performance in directories with > 10000 files. [6]

## TECHNICAL SKILLS

**Programming:** Python, R, Bash

**Developer Tools:** Git, LaTeX, PyTorch, TensorFlow, JAX, Slurm

## HONORS & AWARDS

|                                                                                     |                                |
|-------------------------------------------------------------------------------------|--------------------------------|
| <b>Registration scholarship, Canadian AI 2026</b>                                   | April 2026                     |
| <b>Funded Trainee Award, Advanced Machine Learning Training Network, CAN\$15000</b> | December 2025                  |
| <b>Student Travel Award, Theory and Practice of Differential Privacy</b>            | August 2024                    |
| <b>Ph.D. Tuition Award, UBC</b>                                                     | 2021 - 2024                    |
| <b>Outstanding Individual Award, Huawei, AARC</b>                                   | January 2021                   |
| <b>Outstanding Team Award, Huawei, AARC</b>                                         | January 2021                   |
| <b>MSc. International Tuition Award, UBC</b>                                        | September 2017, September 2018 |
| <b>Outstanding International Student Award, UBC</b>                                 | September 2013                 |

## SERVICE

Reviewer. ICML2026, ECCV 2026, CVPR 2026, AAAI2026, NIPS2025, AISTATS2024, NIPS2024

## SELECTED PUBLICATIONS & PATENTS

\* indicates equal contribution

- [1] Zefeng Li\*, **Qiaoyue Tang\***, Mathias Lécuyer, Evan Shelhamer. Private and Stable Test-time Adaptation with Differential Privacy. (In submission to ICML2026).
- [2] **Qiaoyue Tang**, Sepidehsadat Hosseini, Mengyao Zhai, Thibaut Durand, Greg Mori. FairNVT: Improving Fairness via Noise Injection in Vision Transformers. (In submission to TMLR).
- [3] **Qiaoyue Tang**, Alain Zhiyanov, and Mathias Lécuyer. On the Performance of Differentially Private Optimization with Heavy-Tail Class Imbalance. High-dimensional Learning Dynamics (workshop at ICML). 2025.
- [4] Mishaal Kazmi\*, Hadrien Lautreite\*, Alireza Akbari\*, **Qiaoyue Tang\***, Mauricio Soroco, Tao Wang, Sébastien Gambs, Mathias Lécuyer. PANORAMIA: Privacy Auditing of Machine Learning Models without Retraining. The 38th Annual Conference on Neural Information Processing Systems (NeurIPS) 2024.
- [5] **Qiaoyue Tang**, Frederick Shpilevskiy, Mathias Lécuyer. DP-AdamBC: Your DP-Adam Is Actually DP-SGD (Unless You Apply Bias Correction) AAAI 2024 (**Oral**).
- [6] **Qiaoyue Tang**, Mathias Lécuyer. DP-SGD-LF: Improving Utility under Differentially Private Learning via Layer Freezing. Arxiv. 2022.
- [7] **Qiaoyue Tang**, Hailin Hu, Chenwei Liu, Wei Peng. A Bug Localization Method for Software Defect Tracking Systems using Sequence-to-Sequence Techniques. Patent, patent ID: 86883482CN01-203585
- [8] Chenwei Liu, **Qiaoyue Tang**. Triplet Convolutional Networks for Classifying Mixed-Type WBM Patterns with Noisy Labels. 2021 IEEE International Test Conference (ITC).
- [9] **Qiaoyue Tang**. Classification Strategies for High-dimensional Multiclass Imbalanced Data. 2019. *MSc. Thesis*