Qiaoyue Tang

Website: qiaoyuet.github.io
Email: qiaoyuet@cs.ubc.ca
cathy.tangqiaoyue@gmail.com
Google Scholar: Qiaoyue Tang

Research Interests

I combine theoretical and empirical analysis to develop methods for differentially private machine learning, including private optimization, privacy auditing, as well as broader problems in trustworthy AI.

Education

University of British Columbia — Vancouver, Canada
Ph.D. in Computer Science, Advisor: Mathias Lécuyer — 2021 – Present
Expected graduation: Dec 2026
Thesis: Private Machine Learning: Training, Evaluating, and Adapting Models with Differential Privacy

University of British Columbia — Vancouver, Canada
M.Sc. in Statistics, Advisor: Aline Talhouk, Lang Wu — 2017 – 2019
Thesis: Classification Strategies for High-dimensional Multiclass Imbalanced Data

University of British Columbia — Vancouver, Canada
B.Sc. in Statistics — 2013 – 2017

Research Experience

Graduate Research Assistant — Vancouver, Canada
University of British Columbia — 2021 – Present
- Differentially private optimization with improved privacy-utility tradeoff. [4][5][6][7]
- Privacy auditing on trained models. [3]
- Private test-time adaptation under distribution shift. [1]

Machine Learning Research Intern — Vancouver, Canada
Royal Bank of Canada (RBC), Borealis — 2025
- Fair classification from biased pre-trained models. [2]

Machine Learning Engineer — Shenzhen, China
Huawei Technologies, AI Application Research Center — 2019 – 2021
- Design and develop AI solutions for industry use. [8][9][10]

Graduate Research Assistant — Vancouver, Canada
BC Cancer Research Center, OVCARE — 2018 – 2019
- High-dimensional imbalanced classification on gene expression data (Master's Thesis).

Undergraduate Research Assistant — Vancouver, Canada
Vancouver General Hospital, Eye Care Center — 2016
- Statistical analysis on clinical data.

Publications

Shared first authorship is denoted with *.

Conference Proceedings

[1] *Private and Stable Test-time Adaptation with Differential Privacy.*
Zefeng Li*, **Qiaoyue Tang***, Mathias Lécuyer, Evan Shelhamer.
International Conference on Machine Learning (ICML) 2026.

[2] *Improving Fairness via Noise Injection in Vision Transformers.*
Qiaoyue Tang, Sepidehsadat Hosseini, Mengyao Zhai, Thibaut Durand, Greg Mori.
Transactions on Machine Learning Research (TMLR) 2026.

[3] *PANORAMIA: Privacy Auditing of Machine Learning Models without Retraining.*
Mishaal Kazmi*, Hadrien Lautraite*, Alireza Akbari*, **Qiaoyue Tang***, Mauricio Soroco, Tao Wang, Sébastien Gambs, Mathias Lécuyer.
Neural Information Processing Systems (NeurIPS) 2024.
Earlier version at Theory and Practice of Differential Privacy (TPDP) 2024.

[4] *DP-AdamBC: Your DP-Adam Is Actually DP-SGD (Unless You Apply Bias Correction).*
Qiaoyue Tang, Frederick Shpilevskiy, Mathias Lécuyer.
AAAI Conference on Artificial Intelligence (AAAI) 2024. (**Oral, 2.3%**)

Workshop Proceedings

[5] *On the Performance of Differentially Private Optimization with Heavy-Tail Class Imbalance.*
Qiaoyue Tang, Alain Zhiyanov, Mathias Lécuyer.
High-dimensional Learning Dynamics Workshop at ICML 2025.

[6] *DP-Adam: Correcting DP Bias in Adam's Second Moment Estimation.*
Qiaoyue Tang, Mathias Lécuyer.
Trustworthy and Reliable Large-Scale Machine Learning Models (RTML) Workshop at ICLR 2023.

Other Manuscripts

[7] *DP-SGD-LF: Improving Utility under Differentially Private Learning via Layer Freezing.*
Qiaoyue Tang, Mathias Lécuyer.
arXiv preprint, 2022.

[8] *Triplet Convolutional Networks for Classifying Mixed-Type WBM Patterns with Noisy Labels.*
Chenwei Liu, **Qiaoyue Tang**.
IEEE International Test Conference (ITC) 2021.

[9] *Learning to Solve Soft-Constrained Vehicle Routing Problems with Lagrangian Relaxation.*
Qiaoyue Tang, Yangzhe Kong, Lemeng Pan, Choonmeng Lee.
arXiv preprint, 2021.

[10] *A Bug Localization Method for Software Defect Tracking Systems using Sequence-to-Sequence Techniques.*
Qiaoyue Tang, Hailin Hu, Chenwei Liu, Wei Peng.
Patent, ID: 86883482CN01-203585.

Honors and Awards

- Registration scholarship, Canadian AI Conference — April 2026
- Funded Trainee, Advanced Machine Learning Training Network, CAN$15,000 — December 2025
- Student Travel Award, Theory and Practice of Differential Privacy — August 2024
- Ph.D. Tuition Award, University of British Columbia — 2021 – 2024
- MSc. International Tuition Award, University of British Columbia — 2017 – 2019
- Outstanding International Student Award, University of British Columbia — September 2013

Presentations and Talks

- Conference presentation, *Private and Stable Test-time Adaptation with Differential Privacy.* Responsible AI Track, Canadian Conference on AI, Robots & Vision (AI/CRV), May 2026
- Invited seminar talk, *PANORAMIA: Privacy Auditing of Machine Learning Models without Retraining.* RBC Borealis, June 2025.
- Conference presentation, *DP-AdamBC: Your DP-Adam Is Actually DP-SGD (Unless You Apply Bias Correction).*

UBC/CAIDA TrustML Workshop, February 2024.

- Conference presentation, *DP-AdamBC: Your DP-Adam Is Actually DP-SGD (Unless You Apply Bias Correction).* AAAI Conference on Artificial Intelligence (AAAI), February 2024.

Service

- Reviewer: ICML 2026 (Silver Reviewer), NeurIPS 2024–2025, CVPR 2026, AAAI 2025–2026, AISTATS 2024, TMLR.

Teaching and Mentoring

- **Undergraduate Research Mentor**, University of British Columbia 2023–2025
  Mentor undergraduate students on privacy-preserving machine learning projects, including research design, experimentation, and reproducibility.
- **Head Teaching Assistant**, University of British Columbia 2025
  CPSC 340: Machine Learning and Data Mining
- **Teaching Assistant**, University of British Columbia 2016–2019
  STAT 404: Design and Analysis of Experiments
  STAT 302: Introduction to Probability
  STAT 200: Elementary Statistics for Applications