

# Anvith Thudi

anvith.com

✉ anvith.thudi@mail.utoronto.ca

## Education

---

### University of Toronto

*Ph.D. in Computer Science*

**Toronto, ON, Canada**

*Sep. 2022 - ongoing*

- Advisors: Nicolas Papernot and Chris Maddison

### University of Toronto

*B.Sc in Mathematics, Spent Fall 2020 in Engineering Science*

**Toronto, ON, Canada**

*Sep. 2020 - May 2022*

- GPA: 3.92/4.0

### Simon Fraser University

*Concurrent Studies Student (attended while in highschool)*

**Burnaby, BC, Canada**

*Sep. 2017 - May 2020*

- GPA: 4.09/4.33

## Awards and Honours

---

### 2023 Canada Graduate Scholarship-Doctoral: NSERC

- *declined due to Vanier*

### 2023 Vanier Canada Graduate Scholarship: NSERC

- *Rank 1/173 of national round nominees (Ph.D. students in the Natural Sciences or Engineering)*

**Doctoral Entrance Scholarship:** UofT Department of Computer Science

**Doctoral Recruitment Award:** UofT Faculty of Arts and Science

**Galois Award:** University College UofT

**Dean's List Scholar:** UofT

**Dean's Honours List:** UofT

**2020 Loran Scholarship National Finalist:** Loran Scholar's Foundation

- *Top 88 highschool students in Canada*

## Publications

---

### Journal Proceedings.....

**"From Differential Privacy to Bounds on Membership Inference: Less can be More":** *Anvith Thudi, Iliia Shumailov, Franziska Boenisch, Nicolas Papernot. Transactions on Machine Learning Research*

### Conference Proceedings.....

**"Gradients Look Alike: Sensitivity is Often Overestimated in DP-SGD":** *Anvith Thudi, Hengrui Jia, Casey Meehan, Iliia Shumailov, Nicolas Papernot. Proceedings of the 33rd USENIX Security Symposium, 2024*

**"Better Sparsifiers for Directed Eulerian Graphs":** *Sushant Sachdeva, Anvith Thudi, Yibin Zhao. Proceedings of the 51st EATCS International Colloquium on Automata, Languages and Programming*

**"Training Private Models That Know What They Don't Know":** *Stephan Rabanser, Anvith Thudi, Abhradeep Thakurta, Krishnamurthy Dvijotham, Nicolas Papernot. Proceedings of the 37th Conference on Neural Information Processing Systems*

**"Proof-of-Learning is Currently More Broken Than You Think":** *Congyu Fang, Hengrui Jia, Anvith Thudi, Mohammad Yaghini, Christopher A. Choquette-Choo, Natalie Dullerud, Varun Chandrasekaran, Nicolas Papernot. Proceedings of the 8th IEEE European Symposium on Security and Privacy, 2023*

**"On the Necessity of Auditable Algorithmic Definitions for Machine Unlearning"**: Anvith Thudi, Hengrui Jia, Ilia Shumailov, Nicolas Papernot. *Proceedings of the 31st USENIX Security Symposium*, 2022

**"Unrolling SGD: Understanding Factors Influencing Machine Unlearning"**: Anvith Thudi, Gabriel Deza, Varun Chandrasekaran, Nicolas Papernot. *Proceedings of the 7th IEEE European Symposium on Security and Privacy*, 2022

**"Proof of Learning: Definitions and Practice"**: Hengrui Jia, Mohammad Yaghini, Christopher A. Choquette-Choo, Natalie Dullerud, Anvith Thudi, Varun Chandrasekaran, Nicolas Papernot. *Proceedings of the 42nd IEEE Symposium on Security and Privacy*, 2021

## Preprints

---

**"Finding Optimally Robust Data Mixtures via Concave Maximization"**: Anvith Thudi, Chris J. Maddison

**"Unlearnable Algorithms for In-context Learning"**: Andrei Muresanu, Anvith Thudi, Michael R. Zhang, Nicolas Papernot

**"Selective Classification via Neural Training Dynamics"**: Stephan Rabanser, Anvith Thudi, Kimia Hamidieh, Adam Dziedzic, Nicolas Papernot

**"SoK: Machine Learning Governance"**: Varun Chandrasekaran, Hengrui Jia, Anvith Thudi, Adelin Travers, Mohammad Yaghini, Nicolas Papernot

## Experience

---

Microsoft Research Cambridge  
Ph.D. Research Intern

Cambridge, UK  
May. 2023 - July 2023

## Talks

---

**"Datapoints that are Easy to Unlearn"**: Google DeepMind

**"Gradients Look Alike: Sensitivity is Often Overestimated in DP-SGD"**: Usenix Security 24'

**"Datapoints that are Easy to Unlearn"**: Harvard Efficient ML Seminar

**"The Unlearning Problem(s)"**: CS 562 at University of Illinois Urbana-Champaign

**"The Unlearning Problem(s)"**: The Alan Turing Institute

**"The Unlearning Problem(s)"**: Cambridge

**"The Unlearning Problem(s)"**: Google

**"The Unlearning Problem(s)"**: EPFL

**"The Unlearning Problem(s)"**: ETH Zurich

**"On the Necessity of Auditable Algorithmic Definitions for Machine Unlearning"**: Usenix Security 22'

**"Unrolling SGD: Understanding Factors Influencing Machine Unlearning"**: Euro S&P 22'

**"The Unlearning Problem(s)"**: Meta

## Service

---

**Reviewer**: Euro S&P (2022), ICLR (2025)

**Subreviewer**: IEEE S&P (2024), CCS (2023), Neurips (2022)

**Panel**: Neurips 2023 Unlearning Competition