

# 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 Vanier Canada Graduate Scholarship:** NSERC

○ Rank 1/173 of national round nominees (*Ph.D. students in Natural Sciences and 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

### Conference Proceedings

**"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

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

**"Bounding Membership Inference":** **Anvith Thudi**, Ilia Shumailov, Franziska Boenisch, Nicolas Papernot

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

## Experience

---

**Microsoft Research Cambridge**  
*Ph.D. Research Intern*

**Cambridge, UK**  
*May. 2023 - July 2023*

## Talks

---

"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