

# Anvith Thudi

anvith.thudi@mail.utoronto.ca

CS PhD student at UofT. Former Math Specialist student at UofT, and Concurrent Studies Student at SFU (attended while still in high school).

## EDUCATION

### University of Toronto, Toronto - Computer Science PhD

Sep. 2022 - ongoing

Co-advised by Prof. Nicolas Papernot and Prof. Chris Maddison

### University of Toronto, Toronto - Math Specialist Student (BSc)

Jan. 2021 - June 2022 (expected)

GPA: 3.92/4.0

Enrolled in predominantly 4th year/graduate courses, continuing my math education from SFU. Spent 2020 Fall in Engineering Science.

### Simon Fraser University, Burnaby — Concurrent Studies Student

Sept. 2017 - April 2020

GPA: 4.09/4.33

Followed a math major stream while still attending highschool.

## RESEARCH

### Cleverhans Lab (Machine Learning Privacy and Security)

Aug. 2020 (ongoing)

Part of Prof. Nicolas Papernot's lab affiliated with the University of Toronto and Vector Institute

#### Conference Papers:

- 1) "Proof of Learning: Definitions and Practice" *Hengrui Jia, Mohammad Yaghini, Christopher A. Choquette-Choo, Natalie Dullerud, Anvith Thudi, Varun Chandrasekaran, Nicolas Papernot* in Proceedings of the **42nd IEEE Symposium on Security and Privacy**, San Francisco, CA. (2021)
- 2) "On the Necessity of Auditable Algorithmic Definitions for Machine Unlearning" *Anvith Thudi, Hengrui Jia, Ilia Shumailov, Nicolas Papernot* in Proceedings of the **31st USENIX Security Symposium** <https://arxiv.org/abs/2110.11891>
- 1) "Unrolling SGD: Understanding Factors Influencing Machine Unlearning" *Anvith Thudi, Gabriel Deza, Varun Chandrasekaran, Nicolas Papernot* in Proceedings of the **7th IEEE European Symposium on Security and Privacy** <https://arxiv.org/abs/2109.13398?context=cs.C>

#### Preprints:

- 1) "Selective Classification via Neural Training Dynamics" *Stephan*

## AWARDS

**2020 Loran Scholarship**

**National Finalist**

*Rabanser, Anvith Thudi, Kimia Hamidieh, Adam Dziedzic,  
Nicolas Papernot* <https://arxiv.org/abs/2205.13532>

- 2) “Bounding Membership Inference” *Anvith Thudi, Ilya Shumailov,  
Franziska Boenisch, Nicolas Papernot*  
<https://arxiv.org/abs/2202.12232>
- 3) “SoK: Machine Learning Governance” *Varun Chandrasekaran,  
Hengrui Jia, Anvith Thudi, Adelin Travers, Mohammad Yaghini,  
Nicolas Papernot* <https://arxiv.org/abs/2109.10870>

## TALKS

**The Unlearning Problem(s) - Meta**

**Unrolling SGD: Understanding Factors Influencing Machine Unlearning - Euro S&P 22’**

**On the Necessity of Auditable Algorithmic Definitions for Machine Unlearning - Usenix Security 22’**