Sacha Servan-Schreiber

Website: sachaservanschreiber.com
Email: 3s [at] mit.edu
GitHub: github.com/sachaservan

Research interests and vision

My research focuses on designing and building privacy-preserving systems. In doing so, I am interested in developing new theoretical tools that enable better performance for secure computation. I believe that the future of the Internet depends on the development of *efficient* cryptographic tools that improve user privacy and security.

Education

Massachusetts Institute of Technology — Cambridge, MA
Ph.D. in Computer Science — 2019–2025

- Thesis: "New Tools for On-the-Fly Secure Computation"

Massachusetts Institute of Technology — Cambridge, MA
M.S. in Computer Science — 2019–2021

- Thesis: "Private Similarity Search with Sublinear Communication"
- *William A. Martin Master's Thesis Award in Computer Science*

Brown University — Providence, RI
Sc.B in Computer Science (with honors) — 2016–2019

- Thesis: "Cryptographically Certified Hypothesis Testing"

Teaching Experience

Massachusetts Institute of Technology — Cambridge, MA

MEng Supervisor — Fall 2022–Spring 2023

- Mentored a masters student working on applied cryptography research.

MIT PRIMES Mentor — Spring 2020–Spring 2025

- Mentored eight high-school students working on research in cryptography and computer security.

Teaching Assistant — Fall 2021

- 6.875: Foundations of Cryptography; taught by Vinod Vaikuntanathan.

UROP Mentor — Fall 2020–Fall 2021

- Co-mentored an undergraduate student working on research in cryptography and computer security.

Grading Assistant — Fall 2021

- 6.875: Foundations of Cryptography (co-taught with Berkeley CS276).

Brown University — Providence, RI

Undergraduate Teaching Assistant — Fall 2017–Spring 2018

- CS1230: Introduction to Computer Graphics; taught by Andy van Dam.
- CS1800: Cybersecurity and International Relations; taught by John Savage.

Work and Research Experience

Tinfoil — San Francisco, CA
Co-founder — January 2025, Present

- Building privacy-preserving AI with secure hardware enclaves.

NTT Research — Sunnyvale, CA
Research Intern — Summer 2024

- Ph.D. research intern working with Elette Boyle and Abhishek Jain.

IRIF at Université Paris Cité — Paris, France
Visiting Student — Fall 2023, Spring 2024

- Visiting student in Geoffroy Couteau's research lab at IRIF.

Microsoft Research New England — Cambridge, MA
Research Intern — Summer 2023

- Ph.D. research intern working with Yael Kalai.

Brown University — Providence, RI
Research Assistant — January 2017–March 2019

- Undergraduate research assistant in the Database Systems Lab and Visual Computing Lab.

MongoDB — New York, NY
Intern — Summer 2016

- Worked with the MongoDB University team to improve their mobile platform.

Intern & Independent Contractor — June 2015–December 2015

- Designed and built the MongoDB University mobile app from the ground up.

Academic Services

Reviewer

- ACM Transactions on Privacy and Security (TPS) 2022
- Designs, Codes and Cryptography (DESI) 2024

External Reviewer

- International Conference on Practice and Theory in Public Key Cryptography (PKC) 2025
- International Conference on Applied Cryptography and Network Security (ACNS) 2024
- International Symposium on Computer Architecture (ISCA) 2023
- IEEE Symposium on Security and Privacy (Oakland) 2023
- ACM Conference on Computer and Communications Security (CCS) 2021
- Annual International Cryptology Conference (Crypto) 2020

Talks

ArcticCrypt — Svalbard, Norway
Non-Interactive Distributed Point Functions — July 7th 2025

PKC — Røros, Norway
Non-Interactive Distributed Point Functions — May 12th 2025

Eurocrypt — Madrid, Spain
Simultaneous-Message and Succinct Secure Computation — May 8th 2025

Amherst College — Amherst, MA
On-the-Fly Secure Computation — March 25th 2025

MIT Security Seminar — Cambridge, MA
Non-Interactive Distributed Point Functions — March 6th 2025

IRIF laboratory at the University of Paris Cité — Paris, France
QuietOT: Lightweight Oblivious Transfer with a Public-Key Setup — January 14th 2025

Asiacrypt — Kolkata, India
Constrained Pseudorandom Functions for Inner-Product Predicates from Weaker Assumptions — December 13th 2024

Asiacrypt — Kolkata, India
QuietOT: Lightweight Oblivious Transfer with a Public-Key Setup — December 13th 2024

MIT CSAIL Ph.D. Thesis Defense — Cambridge, MA
New Tools for On-the-Fly Secure Computation — December 5th 2024

Tufts University: 2nd Anonymity Day Workshop — Somerville, MA
Robust and Scalable Metadata-Private Anonymous Broadcast — November 15th 2024

Stanford Security Lunch — Palo Alto, CA
Private Analytics: Challenges in Real-World Deployments — June 26th 2024

NTT CIS Seminar — Sunnyvale, CA
Constrained Pseudorandom Functions for Inner-Product Predicates from Weaker Assumptions — June 25th 2024

MIT Security Seminar — Cambridge, MA
Constrained Pseudorandom Functions for Inner-Product Predicates from Weaker Assumptions — April 25th 2024

MIT CSAIL + Imagination in Action: AI Frontier & Implications — Cambridge, MA
How to Have a Private Conversation with AI — June 26th 2023

IEEE Symposium on Security and Privacy — San Francisco, CA
Private Access Control for Function Secret Sharing — May 22nd 2023

IRIF laboratory at the University of Paris Cité — Paris, France
Private Access Control for Function Secret Sharing — January 10th 2023

IEEE Symposium on Security and Privacy — San Francisco, CA
Private Approximate Nearest Neighbor Search with Sublinear Communication — May 24th 2022

Symposium on Networked Systems Design and Implementation — Renton, WA
Spectrum: High-bandwidth anonymous Broadcast — April 4th 2022

Berkeley University — Virtual
Private Approximate Nearest Neighbor Search with Sublinear Communication — February 18th 2022

Cornell University — Virtual
AdVeil: A Private Targeted Advertising Ecosystem — September 21st 2021

Brave Research — Virtual
AdVeil: A Private Targeted Advertising Ecosystem — September 15th 2021

Northeastern University — Virtual
AdVeil: A Private Targeted Advertising Ecosystem — September 1st 2021

Northeastern University — Virtual
Spectrum: High-bandwidth anonymous Broadcast — July 7th 2021

Cornell University — Virtual
Spectrum: High-bandwidth anonymous Broadcast — March 11th 2021

Scholarships and Awards

- William A. Martin Master's Thesis Award — 2021
- Jacobs Foundation Research Fellowship — 2019
- ICDM Best Student Paper Runner-up — 2018