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 apply existing cryptographic primitives and develop new theoretical tools that enable better performance and security in anonymous communication, recommendation systems, and private databases. I believe that the future of the Internet depends on the development of cryptographic tools that improve user privacy and security.

Education

Massachusetts Institute of Technology — Cambridge, MA
Ph.D. Candidate — 2019–Current

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–Current

- Currently co-mentor two 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.

Current and past students

Albert Lu (co-mentored with Jules Drean; MIT PRIMES)

Andrew Carratu (co-mentored with Jules Drean; MIT PRIMES)

Eli Yablon (MIT PRIMES → Princeton undergrad)

Simon Beyzerov (MIT PRIMES → CMU undergrad)

Hyojae Park (MIT PRIMES → CMU undergrad)

Pawan Goyal (MEng → Two Sigma)

Srijon Mukherjee (co-mentored with Zack Newman; MIT UROP → D.E. Shaw)

Patrick Zhang (co-mentored with Kyle Hogan; MIT PRIMES → MIT undergrad)

Work and Research Experience

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 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

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 — 2019–2020
- ICDM Best Student Paper Runner-up — 2018

Publications

[1] S. Langowski, **S. Servan-Schreiber**, and S. Devadas, "Trellis: Robust and scalable metadata-private anonymous broadcast", in *2023 Network and Distributed System Security (NDSS) Symposium*, 2023.

[2] **S. Servan-Schreiber**, S. Beyzerov, E. Yablon, and H. Park, "Private access control for function secret sharing", in *2023 IEEE Symposium on Security and Privacy (S&P)*, IEEE, 2023.

[3] S. Devadas, S. Langowski, N. Samardzic, **S. Servan-Schreiber**, and D. Sanchez, "Designing hardware for cryptography and cryptography for hardware", in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 1–4.

[4] K. Hogan, **S. Servan-Schreiber**, Z. Newman, B. Weintraub, C. Nita-Rotaru, and S. Devadas, "Shortor: Improving tor network latency via multi-hop overlay routing", in *2022 IEEE Symposium on Security and Privacy (S&P)*, 2022, pp. 1933–1952.

[5] Z. Newman, **S. Servan-Schreiber**, and S. Devadas, "Spectrum: High-bandwidth anonymous broadcast", in *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*, 2022, pp. 229–248.

[6] **S. Servan-Schreiber**, S. Langowski, and S. Devadas, "Private approximate nearest neighbor search with sublinear communication", in *2022 IEEE Symposium on Security and Privacy (S&P)*, IEEE, 2022, pp. 911–929.

[7] T. Kraska, M. Stonebraker, M. Brodie, **S. Servan-Schreiber**, and D. Weitzner, "SchengenDB: A data protection database proposal", in *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, Springer, 2019, pp. 24–38.

[8] **S. Servan-Schreiber**, M. Riondato, and E. Zgraggen, "ProSecCo: Progressive sequence mining with convergence guarantees", *Knowledge and Information Systems*, vol. 62, no. 4, pp. 1313–1340, 2019.

[9] Y. Chung, **S. Servan-Schreiber**, E. Zgraggen, and T. Kraska, "Towards quantifying uncertainty in data analysis & exploration.", *IEEE Data Eng. Bull.*, vol. 41, no. 3, pp. 15–27, 2018.

[10] **S. Servan-Schreiber**, M. Riondato, and E. Zgraggen, "ProSecCo: Progressive sequence mining with convergence guarantees", in *2018 IEEE International Conference on Data Mining (ICDM)*, 2018, pp. 417–426.