

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.

WORK AND RESEARCH EXPERIENCE

NTT Research Research Intern – Ph.D. research intern working with Elette Boyle and Abhishek Jain.	Sunnyvale, CA Summer 2024
IRIF at Université Paris Cité Visiting Student – Visiting student in Geoffroy Couteau’s research lab at IRIF.	Paris, France Fall 2023, Spring 2024
Microsoft Research New England Research Intern – Ph.D. research intern working with Yael Kalai.	Cambridge, MA Summer 2023
Brown University Research Assistant – Undergraduate research assistant in the Database Systems Lab and Visual Computing Lab.	Providence, RI January 2017–March 2019
MongoDB Intern – Worked with the MongoDB University team to improve their mobile platform.	New York, NY Summer 2016
Intern & Independent Contractor – Designed and built the MongoDB University mobile app from the ground up.	June 2015–December 2015

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

<i>Stanford Security Lunch</i> Private Analytics: Challenges in real-world deployments	Palo Alto, CA June 26th 2024
<i>NTT CIS Seminar</i> Constrained Pseudorandom Functions for Inner-Product Predicates from Weaker Assumptions	Sunnyvale, CA June 25th 2024
<i>MIT Security Seminar</i> Constrained Pseudorandom Functions for Inner-Product Predicates from Weaker Assumptions	Cambridge, MA April 25th 2024

<i>MIT CSAIL + Imagination in Action: AI Frontier & Implications</i> How to have a private conversation with AI	Cambridge, MA June 26th 2023
<i>IEEE Symposium on Security and Privacy</i> Private Access Control for Function Secret Sharing	San Francisco, CA May 22nd 2023
<i>IRIF laboratory at the University of Paris Cité</i> Private Access Control for Function Secret Sharing	Paris, France January 10th 2023
<i>IEEE Symposium on Security and Privacy</i> Private Approximate Nearest Neighbor Search with Sublinear Communication	San Francisco, CA May 24th 2022
<i>Symposium on Networked Systems Design and Implementation</i> Spectrum: High-bandwidth anonymous Broadcast	Renton, WA April 4th 2022
<i>Berkeley University</i> Private Approximate Nearest Neighbor Search with Sublinear Communication	Virtual February 18th 2022
<i>Cornell University</i> AdVeil: A Private Targeted Advertising Ecosystem	Virtual September 21st 2021
<i>Brave Research</i> AdVeil: A Private Targeted Advertising Ecosystem	Virtual September 15th 2021
<i>Northeastern University</i> AdVeil: A Private Targeted Advertising Ecosystem	Virtual September 1st 2021
<i>Northeastern University</i> Spectrum: High-bandwidth anonymous Broadcast	Virtual July 7th 2021
<i>Cornell University</i> Spectrum: High-bandwidth anonymous Broadcast	Virtual 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. Zraggen, “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. Zraggen, 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. Zraggen, “ProSecCo: Progressive sequence mining with convergence guarantees”, in *2018 IEEE International Conference on Data Mining (ICDM)*, 2018, pp. 417–426.