Sameer Wagh

Remote – Manhattan, New York
+1 (xxx) xxx-xx33 • snwagh@gmail.com • snwagh.github.io
sameer-wagh • snwagh • sameer.wagh

Professional Summary

I am the Founder of SecretBit Ventures, a technology consulting company and a Senior Research Engineer at OpenMined. Prior to that, I served as the technical leadership at Devron, a distributed data science platform focusing on enterprise setting privacy. I led the R&D arm of Devron, bootstrapping new product verticals – vertical federated learning algorithms, privacy portals, LLM-based privacy analysis – all the way from prototyping to integration into the product, while also managing day-to-day engineering efforts along with the C-suite.

I also spent close to a decade in academia in the space of applied cryptography and privacy enhancing technologies. I have expertise in multi-party computation, homomorphic encryption, federated learning, differential privacy, and developing cryptographic protocols to enable secure computation on sensitive data. I have worked on both the theoretical algorithms as well as end-to-end implementations of these systems. Some of my work has been the choice protocols for open source software and startups in the space. My strong foundation in Mathematics, background in theoretical Physics, and experience in computer science makes me uniquely creative in my problem-solving under constraints, and I look for interesting opportunities to tackle complex challenging problems in a high functioning workplace.

Employment

Mar 2024 – Present
Senior Research Engineer
OpenMined

Oct 2021 – Oct 2023
Head of Privacy
Devron Corporation

July 2020 – Jan 2022
Postdoctoral Researcher
University of California, Berkeley

Education

Sept 2014 – May 2020
Doctor of Philosophy
Electrical Engineering
Princeton University

Aug 2010 – May 2014
B.Tech with Honors
Engineering Physics
Indian Institute of Technology, Madras

Honors and Awards

May 2020: Finalist for the Bede Liu Best Dissertation Award 2020.

Feb 2020: Recipient of the Facebook Systems for ML research award.

June 2019: Winner of the Qualcomm Innovation Fellowship, North America region.

July 2009: Recipient of the P.L. Bhatnagar Memorial Award, as the top scorer of the Indian team at IMO.

July 2009: **Silver Medalist** and India's highest scorer at the 50th International Maths Olympiad, Germany.

Dissertation

Sameer Wagh. "New Directions in Efficient Privacy-Preserving Machine Learning."
PhD Dissertation 2020.
[PDF]

Publications

- Hyesun Kwak, Dongwon Lee, Yongsoo Song, Sameer Wagh. "A General Framework of Homomorphic Encryption for Multiple Parties with Non-Interactive Key-Aggregation"
  International Conference on Applied Cryptography and Network Security (ACNS) 2024

[PDF]

- Mayank Rathee, Conghao Shen, Sameer Wagh, and Raluca Ada Popa. "ELSA: Secure Aggregation for Federated Learning with Malicious Actors"
  IEEE Symposium on Security and Privacy 2023.
  [PDF]
- Jean-Luc Watson, Sameer Wagh, Raluca Ada Popa. "Piranha: A GPU Platform for Secure Computation."
  USENIX Security Symposium 2022.
  [PDF] [Artifact & Code]
- Sameer Wagh. "Pika: Secure Computation using Function Secret Sharing over Rings."
  Privacy Enhancing Technologies Symposium (PETS) 2022. Acceptance Rate: 24%
  [PDF]
- Sameer Wagh. "BarnOwl: Secure Comparisons using Silent Pseudorandom Correlation Generators"
  Tech Report, 2022.
  [PDF]
- Hyesun Kwak*, Dongwon Lee*, Yongsoo Song*, Sameer Wagh*. "A Unified Framework of HE for Multiple Parties with Non-Interactive Setup."
  Under submission
  [PDF] *author list alphabetical
- David Marco Sommer, Liwei Song, Sameer Wagh, and Prateek Mittal. "Towards Probabilistic Verification of Machine Unlearning."
  Privacy Enhancing Technologies Symposium (PETS) 2022. Acceptance Rate: 24%
  [PDF] [Source Code]
- Eleftheria Makri*, Dragoș Rotaru*, Frederik Vercauteren*, Sameer Wagh*. "Rabbit: Efficient Comparison for Secure Multi-Party Computation."
  Financial Cryptography and Data Security (FC) 2021. Acceptance Rate: 25.3%
  [PDF] [Source Code] *author list alphabetical
- Sameer Wagh, Shruti Tople, Fabrice Benhamouda, Eyal Kushilevitz, Prateek Mittal, and Tal Rabin. "Falcon: Honest-Majority Maliciously Secure Framework for Private Deep Learning."
  Privacy Enhancing Technologies Symposium (PETS) 2021. Acceptance Rate: 17%
  [PDF] [Qualcomm Award] [Facebook Award] [News] [News] [Google GSoC, Writeup][Source Code]
- Hao Chen*, Miran Kim*, Ilya Razenshteyn*, Dragoș Rotaru*, Yongsoo Song*, and Sameer Wagh*. "Maliciously Secure Matrix Multiplication with Applications to Private Deep Learning."
  International Conference on the Theory and Application of Cryptology and Information Security (AsiaCrypt) 2020. Acceptance Rate: 25.9%
  [PDF] [Source Code] *author list alphabetical
- Sameer Wagh, Xi He, Ashwin Machanavajjhala, Prateek Mittal. "DP-Cryptography: Marrying Differential Privacy and Cryptography in Emerging Applications."
  Communications of the ACM (CACM) 2020.
  [PDF]
- Sameer Wagh, Divya Gupta, and Nishanth Chandran. "SecureNN: 3-Party Secure Computation for Neural Network Training."
  Privacy Enhancing Technologies Symposium (PETS) 2019. Acceptance Rate: 22%
  [PDF] [Source Code] [Deployment at Cape Privacy] [Deployment at OpenMined]
- Gerry Wan, Aaron Johnson, Ryan Wails, Sameer Wagh, and Prateek Mittal. "Guard Placement Attacks on Path Selection Algorithms for Tor."
  Privacy Enhancing Technologies Symposium (PETS) 2019. Acceptance Rate: 22%
  [PDF] [Source Code]
- Hans Hanley, Yixin Sun, Sameer Wagh, Prateek Mittal. "DPSelect: A Differential Privacy Based Guard Relay Selection Algorithm for Tor."

Privacy Enhancing Technologies Symposium (PETS) 2019. Acceptance Rate: 22%
[PDF]

- Sameer Wagh, Paul Cuff and Prateek Mittal. "Differentially Private Oblivious RAM."
  Privacy Enhancing Technologies Symposium (PETS) 2018. Acceptance Rate: 16%
  [PDF] [Source Code] [News]
- Manuel Costa, Lawrence Esswood, Olya Ohrimenko, Felix Schuster, and Sameer Wagh, "The Pyramid Scheme: Oblivious RAM for Trusted Processors."
  Tech Report, 2017.
  [PDF]
- Yanqi Zhou, Sameer Wagh, Prateek Mittal and David Wentzlaff, "Camouflage: Memory Traffic Shaping to Mitigate Timing Attacks."
  International Symposium on High-Performance Computer Architecture (HPCA) 2017. Acceptance Rate: 22.3%
  [PDF]

Patents

Code Analysis for Sensitive Data using LLMs **September 2023**
Sameer Wagh, Kartik Chopra, and Sid Roy
Under submission

Federated Learning Platform and Methods for using same **August 2022**
Sameer Wagh, Kartik Chopra, and Sid Roy
Patent number: 18/447,874

Private Deep Neural Network Training **February 2018**
Sameer Wagh, Divya Gupta, and Nishanth Chandran
Patent number: 403629-US-PSP / SLW Ref: 1777.778PRV

Tunable Oblivious RAM **January 2015**
Sameer Wagh, Paul Cuff, and Prateek Mittal
Patent number: US20170185534 A1

Work Experience

Head of Privacy, Devron Corporation **2021-2023**
Technical leadership with split focus between research and engineering

Research Internship at Microsoft Research, Redmond, USA **Summer 2019**
Privacy preserving analytics for machine learning

Internship in Applied MPC and Implementations, Bar Ilan University, Israel **Summer 2018**
Implementing efficient MPC primitives and protocols.

Research Internship at Microsoft Research, Bangalore, India **Summer 2017**
Developed efficient cryptographic protocols for privacy preserving machine learning.

Research Internship at Microsoft Research, Cambridge, UK **Summer 2016**
Efficient ORAM protocol implementation in a secure processor environment (SGX).

Research Assistant at Princeton University **Fall 2014**
Differentially Private Oblivious RAM protocol design and implementation

B.Tech Project at IIT Madras **2013-2014**
Quench dynamics across a first order transition in Ashkin Teller model.

Nurture Program by NBHM at TIFR, Bombay. **2011-2013**
BSc equivalent study in pure Mathematics (Algebra, Analysis and Topology)

Research Internship at Okinawa Institute of Science and Technology, Japan **Summer 2013**
Theoretical imaging of magnetic monopoles in frustrated spin-ice systems.

Research Internship at Indian Institute of Science Education and Research, Pune **Summer 2012**
Exploring magnetic traps to manipulate Bose Einstein Condensates.

Research Internship at Oneirix Labs, Pune, India **Summer 2012**
Efficient signal processing for noise cancellation.

Teaching and Mentoring

Mentoring Graduate Students **2020-2021**
Mentoring graduate students at UC Berkeley for academic years 2020 and 2021.

- Mayank Rathee
- Jean-Luc Watson

Mentoring Senior Independent Work **2017-2019**
Mentoring senior independent work at Princeton for academic years 2017, 2018, and 2019.

- Tom Shen: Currently pursuing Masters at UC Berkeley.
- Gerry Wan: Winner of the Calvin Dodd MacCracken Senior Thesis award. Currently pursuing doctorate at Stanford University.
- Hans Hanley: Winner of the Daniel M. Sachs Class of 1960 Graduating Scholarship. Currently pursuing masters at Oxford University.

Teaching Assistant for ELE 535 **Fall 2015**
Teaching assistant for "Machine Learning and Pattern Recognition: Introduction to the theory and practice of machine learning."

Prison Teaching Initiative **2017-2019**
Initiative to reduce incarceration rates by increasing access to post-secondary education. I've taught the following courses at the Garden State Youth Correctional Facility:

- Intermediate Algebra (MAT 030)
- Precalculus II (MAT 113)

PH101, MA101 Coaching Initiative **2013-2014**
Initiative to improve the performance of freshmen in introductory Math and Physics courses.

Talks

Data Science Without Data: An industry Perspective

- (Invited) Charles L. and Ann Lee Brown Distinguished Seminar Series, Virginia, USA Dec 2022

Pika: Secure Computation using Function Secret Sharing over Rings

- Privacy Enhancing Technologies Symposium, Australia July 2022

गोपनीयता और संगणना (Privacy and Computation)

- (Invited) Mahatma Gandhi Antarrashtriya Hindi VishwaVidyalaya Feb 2021

Maliciously Secure Matrix Multiplication with Applications to Private Deep Learning

- Theory and Application of Cryptology and Information Security (AsiaCrypt) Dec 2020

The Rise of Privacy Enhancing Technologies

- Microsoft Research. Redmond — Feb 2020
- AI Research Division, JP Morgan — Feb 2020
- Aarhus University — Nov 2019
- Katholieke Universiteit te Leuven (KU Leuven) — Nov 2019
- École Polytechnique Fédérale de Lausanne (EPFL) — Nov 2019
- RISE Lab, University of California, Berkeley — Oct 2019

Private Deep Learning Made Practical

- Qualcomm, San Diego — Oct 2019

SecureNN: 3-Party Secure Computation for Neural Network Training

- Facebook FAIR, New York — Feb 2019
- Google Deepmind, London — Oct 2018
- IBM TJ Watson Research Center — Sep 2018
- Privacy Enhancing Technologies Symposium, Barcelona — July 2018

Differentially Private Oblivious RAM

- Privacy Enhancing Technologies Symposium, Barcelona — July 2018

Understanding the Mysterious: Bitcoin

- INSPIRE Meetings, Electrical Engineering, Princeton — Jan 2016

Consensus and Byzantine Fault Tolerance

- GSS, Math Department, Princeton — Feb 2015

Path Integrals: Techniques and Applications; Quench Dynamics in the Ashkin Teller Model

- Boltzmann Club, IIT Madras — 2012-2014

Introduction to Groups, Group Representation, Character Theory and Applications in Physics

- Advanced Statistical Mechanics of Fields, IIT-Madras — Nov 2013

Fractals: A Measure Theoretic Introduction

- Advanced Dynamical Systems, IIT-Madras — Oct 2012

Volunteer Services

PC Member

- Privacy Enhancing Technologies Symposium (PETS) — 2022
- Privacy Enhancing Technologies Symposium (PETS) — 2021
- Distributed & Privacy Preserving Machine Learning (ICLR Workshop) — 2021
- Privacy-Preserving Machine Learning in Practice (CCS Workshop) — 2020

Peer Reviewing

- Privacy Enhancing Technologies Symposium (PETS) — 2018, 2019, 2020, 2021, 2022
- USENIX Security Symposium (USENIX) — 2016, 2017, 2018, 2019
- IEEE Symposium on Security and Privacy (S&P) — 2019, 2020, 2021
- Network and Distributed System Security Symposium (NDSS) — 2017, 2018
- ACM Conference on Computer and Communications Security (CCS) — 2021

- Practice and Theory in Public Key Cryptography (PKC) 2019, 2020
- Communications of the ACM (CACM) 2020
- Theory and Application of Cryptology and Information Security (AsiaCrypt) 2019
- Theory and Applications of Cryptographic Techniques (EuroCrypt) 2022
- International Conference on Learning Representations (ICLR) 2021
- Neural Information Processing Systems (NeurIps) 2021

Other Interests

Cadaqués MARNATON September 2023

I successfully completed the 2.5km leg of the Cadaqués Marnaton 2023 (Time: 52:11)

Triathlons May 2022-

I enjoy pushing myself through triathlons – Harryman 2022 (Olympic Individual), Wycoff/Franklin Lakes 2022 (Sprint Relay Team A-10, Swim & Run), New York Triathlon 2023 (Olympic Individual).

Long Distance Runs Nov 2022-

I started long distance running with the Princeton Half Marathon (1:57:17)

Escape from Alcatraz, Swim with the Centurions October 2021

I successfully escaped on Alcatraz on October 16th, swim organized by the Water World Swim. I had the honor and privilage to swim on Coach Pedro's 1000th Alcatraz swim (Time: 32:30)

Organizing MelodEE 2017, 2018

Planning and organizing MelodEE, the annual talent show of ELE department, Princeton University.

Soccer Captain, Varsity Team 2012-2013

Led the university soccer team for the Inter IIT's, the annual sports tournament among all the IIT's. Other responsibilities include organizing Sports Fest (IIT Madras's annual sports tournament), Schroeter (Inter hostel tournaments) and all other university level tournaments.