ANUNAY KULSHRESTHA

312 Sherrerd Hall, Princeton, NJ 08540 / (415) 619-2182 / anunay@cs.princeton.edu / kul.sh

EDUCATION

2019– **Ph.D. in Computer Science** · **Princeton University** · **Center for Information Technology Policy**
Advisor: Prof. Jonathan Mayer

2021 **M.A. in Computer Science** · **Princeton University**

2018 **M.A. in Public Policy** · **Stanford University**
Advisor: Prof. A. Mitchell Polinsky
Thesis: Bittersweet Fruits of Incumbency – Evidence from India (*Advisor*: Prof. Saumitra Jha)

2017 **B.S. in Computer Science** · **Stanford University**
Advisor: Prof. Dan Boneh
Senior Project: Cryptographically Secure Multiparty Computation and Distributed Auctions using Homomorphic Encryption (*Advisor*: Prof. Tim Roughgarden)

2017 **B.S. in Mathematics** · **Stanford University**

PUBLICATIONS

S. Scheffler, **A. Kulshrestha**, J. Mayer. Public Verification for Private Hash Matching: Challenges, Policy Responses, and Protocols, In: *Submission* (Major Revision).

A. Kulshrestha, J. Mayer. Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum, In: *31st USENIX Security Symposium 2022* (to appear).

M. Wang, **A. Kulshrestha**, L. Wang, P. Mittal. Leveraging Strategic Connection Migration-Powered Traffic Splitting for Privacy, In: *Proceedings of the 22nd Privacy Enhancing Technologies Symposium 2022*.

► [Paper] [Best HotPETS 2021 Talk]

A. Kulshrestha, J. Mayer. Identifying Harmful Media in End-to-End Encrypted Communication: Efficient Private Membership Computation, In: *30th USENIX Security Symposium 2021*.

► [Paper] [Presentation] [Slides] [Washington Post] [Boston Globe] [Atlantic] [Forbes]

A. Kulshrestha, A. Rampuria, M. Denton, A. Sreenivas. Cryptographically Secure Multiparty Computation and Distributed Auctions using Homomorphic Encryption, In: *Cryptography*. 2017; 1(3):25.

► [Paper]

A. Kulshrestha, A. Shah, D. Lu. Politically Predictive Potential of Social Networks: Twitter and the Indian General Election 2014, In: *Proc. of the Fourth Multidisciplinary International Social Networks Conference*. ACM, New York, NY, USA.

► [Paper] [Best Paper Award] [Huffington Post] [Hindustan Times].

TALKS

Data Privacy and Policy Implications. U.S. Senate Committee on Commerce (Staff Briefing), November 2021.

Identifying Harmful Media in End-to-End Encrypted Communication. 30th USENIX Security Symposium, August 2021.

Privacy Preserving Health Misinformation Detection. Stanford Internet Observatory E2EE Workshop, March 2021.

Estimating Incidental Collection in Foreign Intelligence Surveillance. Work-in-Progress at CITP, February 2021.

RESEARCH EXPERIENCE

Aug '18–Feb '19 — Research Associate, Prof. Antoinette Schoar (Golub Center for Finance & Policy, MIT Sloan)
▶ *Investigated manipulation in cryptocurrency markets. Studied trading behavior of cryptocurrency miners.*

Apr '18–Jun '18 — Research Assistant, Prof. David Studdert (Center for Health Policy, Stanford)
▶ *Estimated the impact of political partisanship on firearm acquisition during presidential elections using novel data on firearm sale records and precinct-level voting results in California.*

Jul '17–Dec '17
▶ *Examined the effect of firearm acquisition on suicide, homicide & arrest rates in California using a longitudinal cohort by combining weapon registry, voter registry, mortality data, and arrest records.*

Jul '15–Sep '15 — Research Assistant, Prof. Alex Aiken (Computer Science, Stanford)
▶ *Studied the Legion parallel programming system and ported LULESH, a mesh-based framework for simulating fluid dynamics, to Legion.*

Jan '14–Apr '14 — Research Assistant, Prof. Dan Boneh (Computer Science, Stanford)
▶ *Developed one of the first efficient implementations of a private information retrieval protocol in an embedded system using the Paillier cryptosystem.*

AWARDS & GRANTS

2017 Best Paper Award: *Fourth Multidisciplinary International Social Networks Conference, 17-19 July 2017*

2017 Conference Grant: *Awarded by Stanford Undergraduate Advising & Research (UAR)*

2016 Jane Stanford Fellowship for Public Service: *Awarded by the Haas Center for Public Service, Stanford*

2013 Khemka Fellowship: *College scholarship offered to six Indian students studying in the United States*

2013 UC Regents' and Chancellor's Scholarship: *Awarded by UC Berkeley to the top undergraduate applicants*

2012 Best Young Scientist Paper Award: *Awarded by the National Research Council (NRC) Press, Canada*

TEACHING EXPERIENCE

Princeton University

Spring '20–'21 Teaching Assistant, Economics & Computation (COS 445), Prof. Matt Weinberg

Fall '20–'21 Teaching Assistant, Cryptography (COS 433), Prof. Mark Zhandry

Stanford University

Spring '17–'18 Teaching Assistant, Computer and Network Security (CS 155), Prof. Dan Boneh

Winter '17–'18 Teaching Assistant, Introduction to Cryptography (CS 255), Prof. Dan Boneh

Fall '17–'18 Teaching Assistant, Analysis of Networks (CS 224W), Prof. Jure Leskovec
▶ *Mentored research projects analyzing computational, economic or political networks.*

Spring '16–'17 Head Teaching Assistant, Computer and Network Security (CS 155), Prof. Dan Boneh
▶ *Managed a team of 8 TAs and the coordination of a class of over 250 students & industry professionals through the Stanford Center for Professional Development (SCPD).*

PROFESSIONAL EXPERIENCE

Mar '19–Aug '19 Independent Security/Cryptography Consultant (Remote)
▶ *Deployed zero-knowledge proofs and multi-party computation protocols for multiple firms.*

Apr '16–Jul '16 Public Service Fellow, Office of Dr. Shashi Tharoor, Member of Parliament (Thiruvananthapuram, Kerala)
▶ *Designed and developed a civic grievance redressal mechanism for the electorate. Built analytical tools to facilitate evidence-based public policymaking for the MP's office.*

Sep '15–Dec '15 Engineering Intern, Keybase Inc. (San Francisco)
▶ *Developed a secure distributed filesystem for sharing files using public key encryption and implemented secret sharing mechanisms to enable seamless file sharing.*

Jun '14–Sep '14 Research Intern, Search & Discoverability R&D, Bloomberg LP. (New York)
► *Examined re-ranking models for search results and extracted implicit feedback from user metrics. Built infrastructure for interleaving re-ranking models in the HL (Search) function on the Bloomberg Terminal incorporating theoretical insights from recent work in information retrieval. The project was later open sourced as part of the Learning-to-Rank (LTR) plug-in for Apache Solr.*

PROFICIENCY

Programming	C, C++, Go, Rust, Python, R, Haskell
Languages	English (native), Hindi (native), French (beginner)