TRISHA CHADHA DATTA

tcdatta@stanford.edu | https://trishadatta.github.io/

EDUCATION

Stanford University, Stanford, California *Expected Graduation: June 2026*
Ph.D. Computer Science
Adviser: Dan Boneh
Field of Study: Cryptography

Princeton University, Princeton, New Jersey *June 2019*
B.S.E. Computer Science
Departmental GPA: 4.0, Cumulative GPA**:** 3.98, *summa cum laude*

RESEARCH EXPERIENCE

Ongoing Projects

Unique Weighted Threshold Signatures
Stanford University, Stanford, California

- Developing a unique weighted threshold signature scheme based on Chinese Remainder Theorem secret sharing

Publicly Verifiable Secret Sharing Scheme for Field Elements
Aptos Labs, Palo Alto, California

- Developing a publicly verifiable secret sharing scheme for field elements to enable various capabilities (e.g., identity-based encryption, on-chain threshold cryptography, etc.) on the Aptos blockchain

Zero-Knowledge Proofs for Video Edits
Stanford University, Stanford, California

- Demonstrating the feasibility of using zero-knowledge proofs to prove video authenticity by generating zero-knowledge proofs for video edits

Large Language Model Inference on Private Data
Stanford University, Stanford, California

- Developing methods to perform public matrix-private matrix multiplication to enable inference on private data for a public LLM

Past Projects

Mangrove: A Scalable Framework for Folding-based SNARKs
Stanford University, Stanford, California

- Developed a "uniformizing" compiler that converts any poly-time computation into a sequence of identical steps that is especially well-suited to be processed by a

folding-based IVC and additionally developed two optimizations to folding-based IVC

- Developed a SNARK using our uniformizing compiler and optimizations to folding-based IVC that uses a constant-size transparent common reference string, has low memory footprint, is highly parallelizable, and is concretely efficient
- **Published results at CRYPTO 2024**

VerITAS: Verifying Image Transformations at Scale
Stanford University, Stanford, California

- Demonstrated the feasibility of using zero-knowledge proofs to prove photo authenticity by generating zero-knowledge proofs for photo edits (i.e., cropping, editing, and resizing) using Plonky2
- Developed and implemented lattice hashing mechanism for photos
- **Presented results at Real World Crypto 2023**
- **Published results at 2025 IEEE Symposium on Security and Privacy**
- Collaborated with Starling Lab to create zero-knowledge proofs of document redactions for a *Rolling Stone* article, which was nominated for an Emmy for Outstanding Interactive Media

SPINE: Surveillance Protection in the Network Elements
Princeton University, Princeton, New Jersey

- Developed SPINE, a system that leverages programmable switches and the increasing ubiquity of IPv6 in the network core to conceal IP addresses from intermediate (and potentially adversarial) autonomous system
- Developed an encryption scheme to encrypt IP addresses
- Implemented design and encryption mechanism in P4
- **Published results at USENIX Workshop on Free and Open Communications on the Internet (FOCI) co-located with USENIX Security 2019**

Using Word Embeddings to Investigate Bias in Online News and Political Speech
Princeton University, Princeton, New Jersey

- Combined state-of-the-art techniques from natural language processing and psychology to develop a standardized method of measuring bias in large corpora of online news and political speech
- Used word embeddings to calculate a metric that measures where social groups fall along the social dimensions of warmth and competences (i.e., the two social dimensions described by the Stereotype Content Model)

Privacy-Preserving Traffic Obfuscation for Smart Home Devices
Princeton University, Princeton, New Jersey

- Developed mechanisms to obfuscate IoT user activity by shaping TCP traffic flows from IoT devices using packet padding, packet fragmentation, and chaff traffic

- Implemented these mechanisms in a Python library for IoT device developers (available on Github)
- **Presented results at 2018 Federal Trade Commission PrivacyCon Poster Session**
- **Published results at IoT Security and Privacy workshop at 2018 ACM SIGCOMM**

Using SVM for User Profiling for Autonomous Smartphone Authentication
Applied Communication Sciences, Basking Ridge, New Jersey

- Performed research in active authentication to alert users to unauthorized use of their smartphones
- Created app usage features from public data set and used mutual information for feature selection in Java
- Used SVM (LIBSVM library) to learn the app usage behavior of a phone's authorized user
- **Published results at 2015 IEEE MIT Undergraduate Research Technology Conference**

Towards City-Scale Smartphone Sensing of Potentially Unsafe Pedestrian Movements
WINLAB, Rutgers University, North Brunswick, New Jersey

- Created Android apps in Java to record smartphone sensor data
- Developed algorithms to predict when a pedestrian is about to cross a road using sensor data and tested algorithms in MATLAB
- **Published results at HotPlanet workshop, IEEE Mobile Ad hoc and Sensor Systems 2014**

WORK EXPERIENCE

Aptos, Palo Alto, California *June 2024 – August 2024*
Research Intern

- Worked on developing a publicly verifiable secret sharing scheme for field elements to enable various capabilities (e.g., identity-based encryption, on-chain threshold cryptography, etc.) on the Aptos blockchain

Flatiron Health, New York, New York *August 2019 – September 2021*
Software Engineer (E3), Practice Management Team *July 2020 – September 2021*
Software Engineer (E2), Practice Management Team *August 2019 – July 2020*

- Developed features within OncoEMR (Flatiron's electronic health record) to facilitate processes that enable oncology clinics to be reimbursed for treatments

Flatiron Health, New York, New York *Summer 2018*
Software Engineering Intern, Practice Operations Team

- Created feature with C# and Javascript for OncoEMR (Flatiron's electronic health record) to show complete history of an order to allow physicians to understand patient history
- Used Elasticsearch to store and fetch edit history and used React and Redux to render fetched information within OncoEMR

Google, New York, New York *Summer 2017*
Engineering Practicum Intern, Structured Data Team, Research and Machine Intelligence Group

- Designed and implemented an end-to-end machine learning pipeline to predict correlations between fact-checking articles and news articles in Google Search and News
- Generated over 4000 pairs of fact-checking articles and news articles (using Flume and C++) for training data
- Trained ML models that matched fact-checking articles to debunked/verified material and achieved an accuracy rate of 86%

Microsoft, Redmond, Washington *Summer 2016*
Explorer Intern, SQL Engineering and Learning Systems Team

- As a software engineer, created a website with Javascript and HTML to display cost information from multiple databases about internal Azure subscriptions and enable teams to understand and adjust their spending
- As a program manager, oversaw project to create algorithm to predict how many machines were needed for testing to reduce VM resource consumption and save time for engineers

Applied Communication Sciences, Basking Ridge, New Jersey *Summer 2015*
Research Associate

- Performed research in active authentication to alert users to unauthorized use of their smartphones
- **Published results at 2015 IEEE MIT Undergraduate Research Technology Conference**

TEACHING EXPERIENCE

Stanford University, Stanford, CA *Spring 2024*
Co-Instructor for CS 355: Topics in Cryptography

- Lectured and assigned problem sets on topics in modern cryptography including zero-knowledge, multiparty computation, elliptic-curve cryptography, cryptanalysis, privacy, and post-quantum

Princeton University, Princeton, New Jersey *Spring 2018 - Spring 2019*
Lab Teaching Assistant/Grader

- Spring 2019 – COS 461: Computer Networks Grader (graded biweekly assignments and answered online student questions on Piazza)

- Spring 2019 – COS 445: Economics and Computing Undergraduate Teaching Assistant and Grader (held weekly office hours to help students with problem sets and graded biweekly assignments)
- Spring 2018, Fall 2018 – COS 340: Reasoning About Computation Lab Teaching Assistant (held weekly office hours to help students with problem sets)

HONORS/AWARDS

National Awards/Honor Societies

2023 **NSF Graduate Research Fellowship**

2019 **Computing Research Association Outstanding Undergraduate Researcher Honorable Mention**

2018 **Phi Beta Kappa Inductee**

One of 28 members in the Princeton class of 2019 selected for early membership

2017 **Tau Beta Pi Inductee**

Stanford University Awards

2021 **Stanford Graduate Fellowship**

Princeton University Awards

2019 **Phillip Goldman '86 Senior Prize in Computer Science**

Awarded for overall academic excellence, top prize in the Computer Science department

2019 **Outstanding Computer Science Independent Work Prize**

2019 **Sigma Xi Book Award for Outstanding Undergraduate Research**

2019 **Computer Science Department Student Teaching Award**

2018 **Accenture Prize in Computer Science**

Recognizes academic excellence in Computer Science through the end of Junior year

2018 **George B. Wood Legacy Junior Prize**

Awarded during Princeton University Opening Exercises each year to an undergraduate in the senior class in recognition of exceptional academic achievement during their junior year

2017 **Shapiro Prize for Academic Excellence** (for Sophomore Year)

Recognizes ~80 Princeton undergraduates for outstanding academic achievement in their first or second years

PUBLICATIONS

1. **Trisha Datta**, Binyi Chen, Dan Boneh, "VerITAS: Verifying Image Transformations at Scale," in *IEEE Symposium on Security and Privacy*, 2025 (pdf).
2. Wilson Nguyen, **Trisha Datta**, Binyi Chen, Nirvan Tyagi, Dan Boneh, "Mangrove: A Scalable Framework for Folding-based SNARKs," in *CRYPTO*, 2024 (pdf).
3. **Trisha Datta**, Nick Feamster, Jennifer Rexford, Liang Wang, "SPINE: Surveillance Protection in the Network Elements," in Proceedings of the 9th USENIX Workshop on Free and Open Communications on the Internet co-located with USENIX Security, Santa Clara, CA, August 2019 (pdf).

4. **Trisha Datta**, Noah Apthorpe, Nick Feamster, "A Developer-Friendly Library for Smart Home IoT Privacy-Preserving Traffic Obfuscation," in Proceedings of the IoT Security and Privacy Workshop at ACM SIGCOMM, Budapest, Hungary, August 2018 (pdf).

5. **Trisha Datta** and Kyriakos Manousakis, "Using SVM for User Profiling for Autonomous Smartphone Authentication," in Proceedings of the 2015 IEEE MIT Undergraduate Research Technology Conference, Cambridge, MA, 6-8 November 2015 (pdf).

6. **Trisha Datta**, Shubham Jain, Marco Gruteser, "Towards City-Scale Smartphone Sensing of Potentially Unsafe Pedestrian Movements," in Proceedings of the 6th ACM HotPlanet Workshop at IEEE Mobile Ad hoc and Sensor Systems (MASS), Philadelphia, PA, 2014 (pdf).

PRESENTATIONS

1. **Trisha Datta**, "VerITAS: Verifying Image Transformations at Scale", University of Pennsylvania Distributed Systems Laboratory Seminar, Philadelphia, PA, March 2025

2. **Trisha Datta**, "VerITAS: Verifying Image Transformations at Scale", Invited Student Speaker at CSL Conference 2025, Security and Privacy Session, UIUC, IL, February 2025.

3. **Trisha Datta**, "VerITAS: Verifying Image Transformations at Scale", Stanford Security Lunch, Stanford, CA, May 2024.

4. **Trisha Datta**, "VerITAS: Verifying Image Transformations at Scale", SCIEN Seminar, Stanford, CA, May 2024.

5. **Trisha Datta**, "Using ZK to Fight Disinformation," Security Workshop at Stanford Annual Computer Forum, Stanford, CA, April 2024 (link).

6. **Trisha Datta**, "Using ZK Proofs to Fight Disinformation", ZKProofPolicy @ DC, Washington D.C., November 2023 (link).

2. **Trisha Datta**, Dan Boneh, "Using ZK Proofs to Fight Disinformation", Real World Crypto, Tokyo, March 2023 (link).

3. **Trisha Datta**, Noah Apthorpe, Nick Feamster, "Privacy-Preserving Traffic Obfuscation for Smart Home IoT Devices," Federal Trade Commission PrivacyCon Poster Session, Washington D.C., 28 February 2018 (pdf).