Pratik Soni
Assistant Professor,
Kahlert School of Computing, University of Utah,
72 Central Campus Dr, #2863, Salt Lake City, UT 84112.

psoni@cs.utah.edu
https://users.cs.utah.edu/ psoni/
+1 805 886 2175

Research Interests

Cryptography, Theoretical Computer Science, Computer Security. In particular, the design of Zero-knowledge Proofs, Advanced Digital Signature Schemes, and Secure Multi-party Computation.

Research Employment

- **Assistant Professor**, Kahlert School of Computing, University of Utah (July'23 - Present).
- **Postdoctoral Research Fellow**, School of Computer Science, Carnegie Mellon University (CMU) (July'22 - June'23) advised by Prof. Elaine Shi.
- **Postdoctoral Research Fellow**, School of Computer Science, CMU (Nov'20 - June'22) advised by Prof. Vipul Goyal.
- **Research Assistant**, Department of Computer Science, UC Santa Barbara (Jan'16 - Jun'20).
- **Visiting Research Student**, Paul G. Allen School of Computer Science and Engineering, University of Washington, Seattle (Jan'19 - Sep'20).
- **Gradute Fellow**, FACT Center, IDC Herzliya, Israel (Jun'19 - Sep'19).
- **Junior Research Assistant**, School of Computing, National University of Singapore (NUS), Singapore (Jun'14 - May'15).
- **Research Assistant**, Center for Quantum Technologies, NUS, Singapore (May'13 - Jul'13).
- **Research Intern**, Homi Bhabha Center for Science and Education, Tata Institute for Fundamental Research, Mumbai, India (May'12 - Jul'12).

Educational Qualification

- **Ph.D., Computer Science** 2015-2020
  - Thesis: *Transforming Pseudorandomness and Non-malleability with Minimal Overheads*
  - Advisors: Prof. Stefano Tessaro and Prof. Huijia (Rachel) Lin
  - University of California (UC), Santa Barbara, USA
- **M.Sc.(Hons.) Mathematics and B.E.(Hons.) Computer Science** 2010-2015
  - Birla Institute of Technology and Science - Pilani, Goa (India)

Active Grants

1. **RFP-013: Cryptonet Network Grants** - *Stateless Distributed Randomness Generation* - Principal Investigator (USD 11,500).

Proposals in Submission

1. **Sony Focused Research Award** - *Zero-knowledge Proofs for Local Composite Computations: Scalable Provers and Subversion Security* - Principal Investigator (USD 150,000).
2. **Amazon Research Award (AWS Cryptography and Privacy)** - *Scalable Zero-Knowledge Proofs for Local Composite Statements and Applications to Digital Media Provenance* - Principal Investigator (USD 77,859 + USD 8000 AWS credits).
3. **NSF CICI** - *CICI: UCSS: Innovations in Data-Centric Compression and Encryption for Securing Cyberinfrastructure* - Principal Investigator with co-PI Prof. Hari Sundar, University of Utah. (USD 600,000 total; my share USD 300,000).

Proposals in Preparation

1. **NSF SaTC** - *SaTC:BULKVERIFY: A New Technology-Driven Approach to Managing Memory Integrity* - co-Principal Investigator with PI Prof. Rajeev Balasubramonian, University of Utah.
2. **NSF SaTC** - *SaTC: New Frontiers in Zero-Knowledge Proofs* - Principal Investigator.
3. **Stellar Academic Research Grants** - *Fast and Private Solutions for Expressive Blockchain Payments* - Principal Investigator (USD 150,000).

Publications

Authors arranged in alphabetical order(except [C.12])

[C.1] Paul Gerhart, Dominique Schröder, Pratik Soni, Sri AravindaKrishnan Thyagarajan. **Foundations of Adaptor Signatures**, In *Advances in Cryptology - EUROCRYPT 2024, May 2024.*

[C.2] Chen-Da Liu-Zhang, Elisaweta Masserova, João Ribeiro, Mark Simkin, Pratik Soni, Sri AravindaKrishnan Thyagarajan. **Improved YOSO Randomness Generation with Worst-Case Corruptions**, In *Financial Cryptography - FC 2024.*

[C.3] Rex Fernando, Elaine Shi, Pratik Soni, Nikhil Vanjani, Brent Waters. **Non-Interactive Anonymous Router with Quasi-Linear Router Computation**, In *Theory of Cryptography Conference - TCC 2023.*

[C.4] Sourav Das, Rex Fernando, Ilan Komogodsky, Elaine Shi, Pratik Soni. **Distributed-Prover Interactive Proofs**, In *Theory of Cryptography Conference - TCC 2023.*

[C.5] Vipul Goyal, Justin Raizes, Pratik Soni. **Time-Traveling Simulators Using Blockchains and Their Applications**, In *Innovations in Theoretical Computer Science - ITCS 2022, Feb 2022.*

[C.6] Alexandar Block, Justin Holmgren, Alon Rosen, Ron Rothblum and Pratik Soni. **Time- and Space-Efficient Arguments from Groups of Unknown Order**, In *Advances in Cryptology - CRYPTO 2021, Aug 2021.*

[C.7] Alexandar Block, Justin Holmgren, Alon Rosen, Ron Rothblum and Pratik Soni. **Public-Coin Zero-Knowledge Arguments with (almost) Minimal Time and Space Overheads**, In *Theory of Cryptography Conference - TCC 2020, Oct 2020.*

[C.8] Pratik Soni and Stefano Tessaro. **On the Query Complexity of Constructing PRFs from Non-adaptive PRFs**, In *Security and Cryptography for Networks - SCN 2020, Sep 2020.*

[C.9] Pratik Soni and Stefano Tessaro. **Naor-Reingold Goes Public: The Complexity of Known-key Security**, In *Advances in Cryptology - EUROCRYPT 2018, May 2018.*

[C.10] Huijia Lin, Rafael Pass, and Pratik Soni. **Two-Round and Non-Interactive Concurrent Non-Malleable Commitments from Time-Lock Puzzles**,

- In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS), Oct 2017.*
- Invited to the *SIAM Journal of Computing, special issue for top FOCS 2017.*

[C.11] Pratik Soni and Stefano Tessaro. **Public-seed Pseudorandom Permutations**, In *Advances in Cryptology - EUROCRYPT 2017, May 2017.*

[C.12] Pratik Soni, Enrico Budianto, and Prateek Saxena. **The SICILIAN Defense: Signature-based Whitelisting of Web JavaScript**, In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS), Oct 2015.*

Manuscripts in Submission

Authors arranged in alphabetical order

[S.1] Prabhanjan Ananth, Gilad Asharov, Vipul Goyal, Hadar Kaner, Pratik Soni, Brent Waters. **NIZKs with Maliciously Chosen CRS: Subversion Advice Zero-Knowledge and Accountable Soundness**.

[S.2] Pratik Soni, Sri AravindaKrishnan Thyagarajan. **Game-Theoretically Fair Distributed Sampling**.

Manuscripts in Preparation

Authors arranged in alphabetical order

[M.1] Rex Fernando, Yuval Gelles, Ilan Komogodsky, Elaine Shi, Pratik Soni. **Secure MPC for Massively Parallel Computations without ZK-SNARKs**.

[M.2] Pratik Soni, Sri AravindaKrishnan Thyagarajan, Nikhil Vanjani. **Fair Functional Payments using Adaptor Signatures and Functional Encryption**.

[M.3] Zihan Hu, Aayush Jain, Elaine Shi, Pratik Soni. **BQP Simulators for Classical Adversaries and their Applications to Secure Computation**.

Awards and Achievements

1. Invited Participant, CRA Career Mentoring Research Workshop, Washington DC (Feb 2024).
2. Paper [C.10] invited to the SIAM Journal of Computing, special issue for FOCS'17.
3. FOCS Student Travel Award 2017 (600 USD).
4. Merit Scholarship from BITS Pilani, Goa for academic excellence (240,000 INR).
5. Selected for Microsoft India Internship, 2015 (7 students selected out of 250 applicants) - (declined).
6. Selected for NUS-India Research Initiative Summer Internship, 2013.

Invited Talks

1. **Cryptography for Fairness in Distrustful Collaborations and Countering Disinformation** at Utah Data Science Seminar, Jan'24.
2. **Foundations of Advanced Cryptography**
   - New Jersey Institute of Technology, Newark, USA Feb'22.
   - Rensselaer Polytechnic Institute, Troy, USA, Feb'22.
   - Rochester Institute of Technology, Rochester, USA, Feb'22.
   - George Mason University, Washington D.C., USA, Feb'22.
   - University of Utah, Salt Lake City, USA, Mar'22.
3. **Time- and Space-Efficient Arguments from Groups of Unknown Order**,
   - CMU Cryptography Seminar, Jun'21.
   - University of Washington Cryptography Seminar, Jun'21.
   - IST Austria Cryptography Seminar, Jun'21.
   - Cornell University Cryptography Seminar, July'21.
   - John Hopkins Cryptography Seminar, Aug'21.
   - TU Darmstadt & University of Warsaw Seminar on Cryptography & Blockchains, Sep'21.
   - Information-Security Seminar, Royal Holloway University of London, Oct'21.
   - BUSec Seminar, Boston University, Dec'21.

Conference Talks

1. **Time-Traveling Simulators Using Blockchains And Their Applications**, ITCS 2022.
2. **Public-Coin Zero-Knowledge Arguments with (almost) Minimal Time and Space Overheads**, TCC 2020.
3. **On the Query Complexity of Constructing PRFs from Non-adaptive PRFs**, SCN 2020.
4. **Naor-Reingold Goes Public: The Complexity of Known-key Security**, EUROCRYPT 2018.
5. **Two-Round and Non-Interactive Concurrent Non-Malleable Commitments from Time-Lock Puzzles**, FOCS 2017.
6. **Public-Seed Pseudorandom Permutations**, EUROCRYPT 2017.
7. **Thwarting Man-in-the-middle Attacks**, Grad-Slam,[1] UC Santa Barbara, USA, Apr'17.

[1] University-wide competition for the best three-minute talk by a graduate student

Teaching

- University of Utah

Sem	Course	Students	Resp Rate	Instr Avg (KSoC)	Course Avg (KSoC)	Notes
F23	CS5961:Modern Cryptography	4	100%[2]	NA[3]	NA[4]	New Course
F23	CS6961:Modern Cryptography	6	100%	5 (5.21)	5.33 (5.12)	New Course
S24	CS2100:Discrete Structures	211	TBD	TBD	TBD	Co-teaching

- Teaching Assistant at UC Santa Barbara for CS138: Automata and Formal Languages (Fall'15)
- Teaching Assistant at BITS Pilani Goa for Graphs and Networks (Spring'14), Engineering Mathematics (Fall'13), Computer Programming (Spring'13, Spring'12).

Current Advisees

1. Sarabjeet Singh, Ph.D. Candidate at University of Utah (Thesis Committee Member)
2. Ganesh Dhamardhikari, Ph.D. Student at University of Utah (Advisee)
3. Toshihiro Mowery, Undergraduate Student at University of Utah (Advisee)
4. Paul Gerhart, Ph.D. Student at Friedrich-Alexander-University (Thesis Committee Member)
5. Rohit Chatterjee, Ph.D. Student at Sony Brook University (Thesis Committee Member)
6. Nikhil Vanjani, Ph.D. Student at Carnegie Mellon University (Mentor)

Academic and External Service

- Program Committee Member
  - CRYPTO 2024
  - EUROCRYPT 2024
  - ACM CCS 2022 (Applied Cryptography Track)
  - ASIACRYPT 2022
- External Reviewer
  - 2024: ITCS.
  - 2023: TCC.
  - 2022: ITCS, TCC, IEEE Transactions on Information Theory.
  - 2021: CRYPTO, TCC, Journal of Cryptology.
  - 2020: EUROCRYPT, ITC, CRYPTO, TCC.
  - 2019: EUROCRYPT, CRYPTO.
  - 2018: CRYPTO, TCC.
  - 2017: CRYPTO, ASIACRYPT, TCC.
  - 2016: SCN, TCC (2016-B).
- Organizer, *Watch-A-Talk-Together* series at CMU on quantum cryptography.
- Organizational Czar, Cryptography reading group at University of Washington, Seattle (Jan'19-May'19).
- Elected Member, UC Santa Barbara CS Senate (2016-17).
- Co-organizer, *Theory meetups* and Cryptography reading group at UC Santa Barbara.
- Student In-Charge, International Programmes and Collaboration Division, BITS Pilani, Goa.
- Secretary, *Mathletes* - Mathematics Association at BITS Pilani Goa (2012-13).
- Organizer, *Numb3rs* - A competitive mathematics event held at the technical festival *Quark* of BITS Pilani Goa (2013).

Internal Service

1. Member, Graduate Admissions Committee, Fall 2024.
2. Mentor under the First Year PhD Mentoring Program.
   - Aman Sinha, Ph.D. Student.
   - Kunnong Zeng, Ph.D. Student.
3. Organizer, InterMountain Theory Day, tentatively in Summer 2025 (in planning).

Outreach Activities

- Member, Abhigyaan, *A literacy drive which aims at providing 'Education for all'* at Goa, India.
- Guest Speaker at K-12 Outreach Program conducted by the cryptography group at UW CSE.

[2] response rate monitored by the instructor
[3] threshold not met
[4] threshold not met