Dakshita Khurana

Email: dakshita@illinois.edu. **WebURL:** https://www.dakshitakhurana.com/

Research Interests: Cryptography, Quantum Information, Theoretical Computer Science.

Employment

- 2019 – … **University of Illinois Urbana-Champaign;**
  Assistant Professor of Computer Science.
- 2018 – 19 **Microsoft Research, New England;**
  Postdoctoral Researcher.
- 2018 – 19 **University of Illinois Urbana-Champaign;**
  Adjunct Assistant Professor of Computer Science.

Education

- 2018 **Ph.D. in Computer Science** at the University of California, Los Angeles.
- 2014 **M.S. in Computer Science** at the University of California, Los Angeles.
- 2012 **B. Tech. in Electrical Engineering with a Minor in Computer Science** at the Indian Institute of Technology (IIT) Delhi, India.

Honors

- 2024 Google Research Scholar Award
- Dean's Award for Excellence in Research, UIUC.
- 2023 NSF CAREER Award.
- Visa Faculty Research Award.
- On the List of Teachers Ranked as Excellent for Spring 2023.
- 2022 DARPA Forward Riser.
- Visa Faculty Research Award.
- IIT Delhi Graduate of Last Decade (GOLD) Alumni Award.
- On the List of Teachers Ranked as Excellent for Fall 2022.
- 2021 Visa Faculty Research Award.
- On the List of Teachers Ranked as Excellent for Spring 2021.
- *One-way Functions imply Secure Computation in a Quantum World* invited to Quantum Information Processing (QIP)'21 as a Long Plenary Talk.
- 2020 On Forbes' List of 30 under 30 in Science.
- Google Research Fellow at the Simons Institute for the Theory of Computing, Berkeley.
- 2019 On the List of Teachers Ranked as Excellent for Fall 2019.

Honors (continued)

◇ *Weak Zero-knowledge Beyond the Black-box Barrier* invited to the SIAM J. Computing Special Issue for STOC 2019.

2018 ◇ UCLA CS Outstanding Graduating PhD Student Award.

◇ Dissertation Year Fellowship, University of California Los Angeles.

◇ Symantec Outstanding Graduate Student Research Award.

2017 ◇ *How to Achieve Non-malleability in One or Two Rounds* invited to the SIAM J. Computing Special Issue for FOCS 2017.

◇ CISCO Outstanding Graduate Student Research Award.

◇ Invited as Young Researcher to the Heidelberg Laureate Forum.

◇ Invited Participant at Rising Stars in EECS 2017 at Stanford.

2012 ◇ Computer Science Department Fellowship, University of California Los Angeles.

Current and Prior Research Support

2024 ◇ **Google Research Scholar Award**
"Cryptography for the Quantum Age".
PI: Dakshita Khurana. *USD 60,000.*

2023-28 ◇ **Air Force Office of Scientific Research:**
"Computational Hardness in Quantum Cryptography".
PI: Dakshita Khurana. *USD 649,940.*

2023-28 ◇ **NSF CAREER:**
"Cryptographic Proofs, Outside the Black-Box"
PI: Dakshita Khurana. *USD 538,923.*

2023-26 ◇ **NSF SaTC Small:**
"New Cryptographic Capabilities for a Quantum World"
PI: Dakshita Khurana. *USD 571,719.*

2021-24 ◇ **Visa Research Faculty Award**
PI: Dakshita Khurana. *USD 225,000.*

2021-24 ◇ **NSF MPS/Physics**
"Pushing the Boundaries of Classical and Quantum Information Processing Toward Enhanced Security and Energy-Efficient Reliability".
PI: Eric Chitambar, co-PIs: Lav Varshney, Dakshita Khurana. *USD 599,912.*

2020-24 ◇ **DARPA**
"SIEVE: New Directions in Post-Quantum Zero-Knowledge".
PI: Amit Sahai, co-PI: Dakshita Khurana. *UIUC subaward: USD 423,422.*

2019-21 ◇ **C3AI DTI, Jump Arches**,
"Secure Federated Learning for Clinical Informatics".
PI: Oluwasanmi Koyejo, co-PIs: William Bond, Dakshita Khurana. *USD 100,000.*

Current and Prior Research Support (continued)

2019-20 ◇ **Jump ARCHES**,
"Secure Federated Learning for Clinical Diagnostics".
PI: Oluwasanmi Koyejo, co-PIs: William Bond, Dakshita Khurana. *USD 60,000.*

All Publications

Authors are in alphabetical order. The following were published after joining UIUC. Student and postdoctoral co-authors (at the time of submission) are indicated with *.

1. Khurana, D. & *Tomer, K. (2024). Commitments from quantum one-wayness. *In Symposium on the Theory of Computing, STOC 2024 and Quantum Information Processing, QIP 2024.*

2. *Bartusek, J., Goyal, V., Khurana, D., Malavolta, G. & *Roberts, B. (2024). Software with certified deletion. *In Advances in Cryptology, EUROCRYPT 2024 and Quantum Information Processing, QIP 2023.*

3. *Bartusek, J. & Khurana, D. (2023). Cryptography with certified deletion. *In Advances in Cryptology, CRYPTO 2023 and Quantum Information Processing, QIP 2023.* **Invited Tutorial at QCrypt 2023.**

4. *Bartusek, J., Khurana, D. & *Poremba, A. (2023). Publicly-verifiable deletion via target-collapsing functions. *In Advances in Cryptology, CRYPTO 2023.*

5. *Bartusek, J., Khurana, D. & Srinivasan, A. (2023). Secure computation with shared EPR pairs (or: How to teleport in zero-knowledge). *In Advances in Cryptology, CRYPTO 2023.*

6. Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2023b). Round-optimal black-box mpc in the plain model. *In Advances in Cryptology, CRYPTO 2023.*

7. *Agarwal, A., *Bartusek, J., Khurana, D. & *Kumar, N. (2023). A new framework for quantum oblivious transfer. *In Advances in Cryptology - EUROCRYPT 2023.*

8. *Garg, R., Khurana, D., *Lu, G. & Waters, B. (2023). On non-uniform security for black-box non-interactive CCA commitments. *In Advances in Cryptology - EUROCRYPT 2023.*

9. Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2023a). Black-box reusable NISC with random oracles. *In Advances in Cryptology - EUROCRYPT 2023.*

10. *Agarwal, A., Alamati, N., Khurana, D., Raghuraman, S. & Rindal, P. (2023). On black-box verifiable outsourcing. *In Theory of Cryptography Conference, TCC 2023.*

11. *Bartusek, J., Khurana, D., Malavolta, G., *Poremba, A. & Walter, M. (2023). Weakening assumptions for publicly-verifiable deletion. *In Theory of Cryptography Conference, TCC 2023.*

12. Khurana, D., Malavolta, G. & *Tomer, K. (2023). Weak zero-knowledge via the Goldreich-Levin theorem. *In Advances in Cryptology, Asiacrypt 2023.*

13. Canetti, R., *Chakraborty, S., Khurana, D., *Kumar, N., Poburinnaya, O. & Prabhakaran, M. (2022). COA-secure obfuscation and applications. *In Advances in Cryptology, EUROCRYPT 2022.*

14. *Hulett, J., *Jawale, R., Khurana, D. & Srinivasan, A. (2022). SNARGS for P from sub-exponential DDH and QR. *In Advances in Cryptography, EUROCRYPT 2022.*

15. Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2022a). Round optimal black-box protocol compilers. *In Advances in Cryptology, EUROCRYPT 2022.*

16. Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2022b). Round-optimal black-box secure computation from two-round malicious ot. *In Theory of Cryptography Conference, TCC 2022.*

17. Badrinarayanan, S., Ishai, Y., Khurana, D., Sahai, A. & Wichs, D. (2022). Refuting the dream XOR lemma via ideal obfuscation and resettable MPC. *In the Information Theory Conference, ITC 2022.*

18. *Jawale, R., Kalai, Y. T., Khurana, D. & *Zhang, R. (2021). SNARGs and PPAD hardness from sub-exponential LWE. *In Symposium on the Theory of Computing, STOC 2021.*

19. *Bartusek, J., *Coladangelo, A., Khurana, D. & *Ma, F. (2021b). One-way functions imply secure computation in a quantum world. *In Advances in Cryptology, CRYPTO 2021.* **Long Plenary at Quantum Information Processing, QIP 2021. Invited Talk at QCrypt 2021. Invited Talk at Information Theoretic Cryptography (ITC) 2022. Invited Tutorial at the UCLA Institute for Pure and Applied Mathematics (IPAM) Graduate Summer School on Post-quantum and Quantum Cryptography.**

20. *Bartusek, J., *Coladangelo, A., Khurana, D. & *Ma, F. (2021a). On the round complexity of two-party quantum computation. *In Advances in Cryptology CRYPTO 2021, Quantum Information Processing QIP 2021, and QCrypt 2021.*

21. *Chatterjee, R., Garg, S., Hajiabadi, M., Khurana, D., *Liang, X., Malavolta, G., Pandey, O. & *Shiehian, S. (2021). Compact ring signatures from Learning with Errors. *In Advances in Cryptology, CRYPTO 2021.*

22. Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2021). On the round complexity of black-box secure MPC. *In Advances in Cryptology, CRYPTO 2021.*

23. Khurana, D. & Srinivasan, A. (2021). Improved computational extractors and their applications. *In Advances in Cryptology, CRYPTO 2021.*

24. *Agarwal, A., *Bartusek, J., Goyal, V., Khurana, D. & Malavolta, G. (2021b). Two-round maliciously secure computation with super-polynomial simulation. *In Theory of Cryptography Conference, TCC 2021.*

25. Khurana, D. (2021). Non-interactive distributional indistinguishability (NIDI) and non-malleable commitments. *In Advances in Cryptography, EUROCRYPT 2021.*

26. Khurana, D. & Waters, B. (2021). On the CCA upgradeability of public-key infrastructure. *In international conference on practice and theory of public-key cryptography PKC 2021.*

27. *Agarwal, A., *Bartusek, J., Goyal, V., Khurana, D. & Malavolta, G. (2021a). Post-quantum multi-party computation. *In Advances in Cryptography, EUROCRYPT 2021.*

28. *Garg, R., Khurana, D., *Lu, G. & Waters, B. (2021). Black-box non-interactive non-malleable commitments. *In Advances in Cryptography, EUROCRYPT 2021.*

29. *Badrinarayanan, S., *Fernando, R., *Jain, A., Khurana, D. & Sahai, A. (2020). Statistical zap arguments. *In Advances in Cryptology, EUROCRYPT 2020*.

30. Garg, A., Kalai, Y. & Khurana, D. (2020). Computational extractors with negligible error in the crs model. *In Advances in Cryptology, EUROCRYPT 2020*.

31. Khurana, D. & *Mughees, M. H. (2020). On statistical security in two-party computation. *In Theory of Cryptography Conference, TCC 2020*.

32. Bitansky, N., Khurana, D. & Paneth, O. (2019). Weak zero-knowledge beyond the black-box barrier. *In Symposium on the Theory of Computing, STOC 2019.* **Published by invitation in the SIAM Journal on Computing (SICOMP), 2022, Special Issue for STOC 2019.**

33. Kalai, Y. T. & Khurana, D. (2019). Non-interactive non-malleability from quantum supremacy. *In Advances in Cryptology, CRYPTO 2019.*

The following were published before joining UIUC.

34. Badrinarayanan, S., Goyal, V., Jain, A., Kalai, Y., Khurana, D. & Sahai, A. (2018). Promise zero-knowledge and its applications to round-optimal MPC. *In Advances in Cryptology, CRYPTO 2018.*

35. Badrinarayanan, S., Kalai, Y., Khurana, D., Sahai, A. & Wichs, D. (2018). Non-interactive delegation for low-space non-deterministic computation. *In Symposium on the Theory of Computing, STOC 2018.*

36. Kalai, Y., Khurana, D. & Sahai, A. (2018). Statistical WI (and more) in two messages. *In Advances in Cryptology, EUROCRYPT 2018.*

37. Badrinarayanan, S., Khurana, D., Sahai, A. & Waters, B. (2018). Upgrading to functional encryption. In *Theory of Cryptography Conference, TCC 2018*.

38. Khurana, D., Ostrovsky, R. & Srinivasan, A. (2018). Round optimal black-box "Commit-and-Prove". In *Theory of Cryptography Conference, TCC 2018*.

39. Khurana, D. & Sahai, A. (2017). How to achieve non-malleability in one or two rounds. *In IEEE Foundations of Computer Science, FOCS 2017.* **Invited to the SIAM Journal on Computing (SICOMP) Special Issue for FOCS 2017.**

40. Jain, A., Kalai, Y. T., Khurana, D. & Rothblum, R. (2017). Distinguisher- dependent simulation in two rounds and its applications. *In Advances in Cryptology, CRYPTO 2017*.

41. Badrinarayanan, S., Khurana, D., Ostrovsky, R. & Visconti, I. (2017). Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs. *In Advances in Cryptology, EUROCRYPT 2017*.

42. Badrinarayanan, S., Goyal, V., Jain, A., Khurana, D. & Sahai, A. (2017). Round optimal concurrent MPC via strong simulation. In *Theory of Cryptography Conference, TCC 2017*.

43. Khurana, D. (2017). Round optimal concurrent non-malleability from polynomial hardness. In *Theory of Cryptography Conference, TCC 2017*.

44. *Bartusek, J., Goyal, V., Khurana, D., Malavolta, G. & *Roberts, B. (2024). Software with certified deletion. *In Advances in Cryptology, EUROCRYPT 2024 and Quantum Information Processing, QIP 2023.*

45. Goyal, V., Khurana, D. & Sahai, A. (2016). Breaking the three round barrier for non-malleable commitments. *In IEEE Annual Symposium on Foundations of Computer Science, FOCS 2016.*

46. Khurana, D., Kraschewski, D., Maji, H. K., Prabhakaran, M. & Sahai, A. (2016). All complete functionalities are reversible. *In Advances in Cryptology, EUROCRYPT 2016.*

47. Khurana, D., Maji, H. K. & Sahai, A. (2016). Secure computation from elastic noisy channels. *In Advances in Cryptology, EUROCRYPT 2016.*

48. Goyal, V., Khurana, D., Mironov, I., Pandey, O. & Sahai, A. (2016). Do distributed differentially-private protocols require oblivious transfer? In *International Colloquium on Automata, Languages, and Programming, ICALP 2016.*

49. Hofheinz, D., Jager, T., Khurana, D., Sahai, A., Waters, B. & Zhandry, M. (2016). How to generate and use universal samplers. In *Advances in Cryptology, ASIACRYPT 2016.*

50. Agrawal, S., Ishai, Y., Khurana, D. & Paskin-Cherniavsky, A. (2015). Statistical randomized encodings: A complexity theoretic view. In *International Colloquium on Automata, Languages, and Programming, ICALP 2015.*

51. Khurana, D., Rao, V. & Sahai, A. (2015). Multi-party key exchange for unbounded parties from indistinguishability obfuscation. In *Advances in Cryptology, ASIACRYPT 2015.*

52. Khurana, D., Maji, H. K. & Sahai, A. (2014). Black-box separations for differentially private protocols. In *Advances in Cryptology, ASIACRYPT 2014.*

Invited Talks

1. How to Certifiably Delete a Secret. **Simons Institute for the Theory of Computing, Workshop on Cryptography from Minimal Assumptions, Berkeley;** *May 2023.*

2. Cryptography with Certified Deletion. **CMU Cylab Cryptography Seminar, Pittsburgh;** *Nov 2022.*

3. Weakening Assumptions in Quantum Cryptography. **Tutorial at the UCLA IPAM Graduate Summer School on Post-quantum and Quantum Cryptography, Los Angeles;** *July 2022.*

4. From Deletion to Secure Computation and Back. **Invited Spotlight Talk at the Information Theoretic Cryptography Conference (ITC), Boston;** *July 2022.*

5. SNARGs from Sub-exponential DDH and QR. **Boston Crypto Day, Boston;** *July 2022.*

6. Quantum Oblivious Transfer from One-way Functions. **Invited Talk at QCrypt, Virtual;** *Aug 2021.*

7. On Removing Interaction in Non-Malleable Commitments. **MIT Cryptography and Information Security (CIS) Seminar, Virtual;** *Apr 2021.*

8. Secure Federated Learning for Clinical Diagnostics with Applications to the COVID-19 Pandemic. **C3.AI DTI Symposium, Virtual;** *Jan 2021.*

9. SNARGs and PPAD Hardness from Sub-exponential LWE. **Tata Institute of Fundamental Research School of Technology and Computer Science Colloquium, Virtual;** *Dec 2020.*

10. Secure Federated Learning for Clinical Diagnostics. **Jump Arches Seminar, Virtual;** *Nov 2020.*

11. Post-quantum Multi-party Computation. **Theory and Practice of Multiparty Computation Workshop (TPMPC) hosted by Aarhus University, Virtual;** *May 2020.*

12. New Techniques in Zero-Knowledge. **Trends in TCS Workshop, TTI Chicago;** *Jan 2020.*

13. Two-Message Statistically Private Arguments. **Simons Institute for the Theory of Computing, Workshop on Probabilistically Checkable and Interactive Proofs, Berkeley;** *Sep 2019.*

14. Weak Zero-Knowledge Beyond the Black-Box Barrier. **Carnegie Mellon University Theory talk, Pittsburgh;** *Jun 2019.*

15. Quantum Advantage and Classical Cryptography. **Charles River Crypto Day at Northeastern University;** *May 2019.*

16. New Techniques to Overcome Barriers in Simulation. **Indian Institute of Technology, Mumbai;** *Dec 2018.*

17. On Cryptographic Proof Systems. **Caltech CMS Theory Seminar, Los Angeles;** *Dec 2017.*

18. New Techniques for Extraction. **South California Theory Day, Los Angeles;** *Nov 2017.*

19. The Virtues of Two-Message OT. **Boston University Crypto Seminar, Boston;** *Sep 2017.*

20. Distinguisher-Dependent Simulation. **DIMACS Workshop on Outsourcing Computation Securely, Rutgers University New Brunswick;** *Jul 2017.*

21. How to Achieve Non-Malleability in One or Two Rounds. **MIT Cryptography and Information Security (CIS) Seminar, Cambridge;** *Jun 2017.*

22. Birthday Simulation from Exponential Hardness, and its Applications. **New York Crypto Day at Cornell Tech, New York;** *May 2017.*

23. Two-Message Non-Malleable Commitments. **UCSD Theory Seminar, San Diego;** *Nov 2016.*

24. How to Generate and Use Universal Samplers. **Stanford DIMACS Workshop on**

Cryptography and Software Obfuscation, Palo Alto; *Nov 2016.*

25. Breaking the Three Round Barrier for Non-Malleable Commitments. **Simons Institute for The Theory of Computing, Cryptography Reunion Workshop, Berkeley;** *Aug 2016.*

26. Breaking the Three Round Barrier for Non-Malleable Commitments. **DIMACS Workshop on Cryptography and its Interactions, Rutgers University, New Brunswick;** *Jul 2016.*

27. How to Obtain Two-Message Non-Malleable Commitments. **MIT Cryptography and Information Security (CIS) Seminar, Cambridge;** *Jun 2016.*

28. Constructing Two-Message Non-Malleable Commitments. **New York University Cryptography Reading Group, New York;** *May 2016.*

29. New Constructions of Non-Malleable Commitments. **Cornell Tech Cryptography Seminar, New York;** *May 2016.*

30. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **Stanford Security Seminar, Palo Alto;** *Feb 2016.*

31. How to Generate and Use Universal Samplers. **South California Theory Day, Los Angeles;** *Nov 2015.*

32. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **Simons Institute for the Theory of Computing, Workshop on Securing Computation, Berkeley;** *Aug 2015.*

Advisees

Postdoc

◇ **Mehrdad Tahmasbi**, 2023-Present.

PhD

◇ **Ruta Jawale**, 2019-Present. (Graduation expected: 2025)

◇ **Amit Agarwal**, 2019-Present. (Graduation expected: 2025)

◇ **James Hulett**, 2020-Present. (Graduation expected: 2026)

◇ **Kabir Tomer**, 2022-Present. (Graduation expected: 2027)

MS

◇ **Nishant Kumar**, MS Completed: 2022.
Thesis: New Frameworks for Quantum Oblivious Transfer.

◇ **Ruta Jawale**, MS Completed: 2022.
Thesis: Succinct Non-interactive Arguments for Bounded Depth Computations.

◇ **Andrew Liu**, MS Completed: 2022.
Thesis: Secure and Scalable Robust Federated Learning.

◇ **Amit Agarwal**, MS Completed: 2021.
Thesis: Two-Round Maliciously Secure Computation with Superpolynomial Simulation.

Undergrad

◇ **Alexandra Levinshtyn,** 2023 - Present.

◇ **Devin Akman**, Graduated: 2020.
Thesis: New Techniques in Non-malleable Secret Sharing for General Structures.
Now PhD student at the Washington University of St. Louis.

Advisees (continued)

- **Kabir Tomer**, Summer intern, 2020.
  Now PhD student at the University of Illinois, Urbana-Champaign.
- **Olivia Figueira**, Summer Distributed REU (DREU) intern, 2020.
  Now PhD student at the University of California, Irvine.

Teaching

Fall 2023
- UIUC. Introduction to Quantum Computing (Undergraduate) CS 498 QC.

Spring 2023
- UIUC. Topics in Cryptography (Graduate) CS 507.
  Listed among Teachers Ranked as Excellent by Their Students.

Fall 2022
- UIUC. Cryptography (Undergraduate) CS 407.
  Listed among Teachers Ranked as Excellent by Their Students.

Spring 2022
- UIUC. Quantum Cryptography (Graduate) CS 598CTO.

Fall 2021
- UIUC. Algorithms and Models of Computation (Undergraduate) CS 374.

Spring 2021
- UIUC. Special Topics in Cryptography (Graduate) CS 598 DK.
  Listed among Teachers Ranked as Excellent by Their Students.

Fall 2020
- UIUC. Applied Cryptography (Undergraduate) CS/ECE 498 AC (407).

Fall 2019
- UIUC. Special Topics in Cryptography (Graduate) CS 598 DK.
  Listed among Teachers Ranked as Excellent by Their Students.

Outreach

Mentorship
- Panelist at the CrossFyre workshop for female cryptography researchers in 2024.
- Mentor and panelist at the Rising Stars in EECS Workshop at UIUC in 2019.
- SafeToC Volunteer, ensuring a safe environment in CS theory conferences including ACM STOC, IEEE FOCS and ITCS; 2020-Present.
- Member of the Broadening Participation in Computing Committee at the UIUC CS Department, 2021-22 (Policy subcommittee), 2022-23 (Engagement subcommittee). Helped shape department policy to facilitate inclusion and retention.
- CS STARS (Student Ambassadors/Research Scholars) mentor to undergraduate female researchers, 2023-Present.
- UIUC IDEA (Inclusion, Diversity, Equity & Access) Institute Affiliate, 2020-Present

External Service

Workshops
- Organizer of the Midwest Crypto Day, 2023-Present
- Co-organizer of the STOC'22 workshop: The Multiple Facets of Quantum Proofs

External Service (continued)

- PC co-chair of the Asiacrypt'22 Satellite workshop on Quantum Cryptography

PC Member

- ACM Symposium on the Theory of Computing (STOC) 2024
- Annual International Cryptology Conference (CRYPTO) 2024
- Innovations in Theoretical Computer Science (ITCS) 2023
- ACM Symposium on the Theory of Computing (STOC) 2022
- Theory of Cryptography Conference (TCC) 2022
- ACM Symposium on the Theory of Computing (STOC) 2020
- Theory of Cryptography Conference (TCC) 2020
- Innovations in Theoretical Computer Science (ITCS) 2020
- International Conference on Cryptology in India (INDOCRYPT) 2020
- IACR Conference on Theory and Applications of Cryptology (EUROCRYPT) 2019

Internal Service

UIUC Engg

- IQUIST (Illinois Quantum Information Science & Technology) Center:
  - Science Advisory Board (SAB) Member, 2021-24
  - Seminar Series Co-organizer, 2021-22
  - Postdoctoral Scholars Program Committee Member, 2022-23

UIUC CS

- Tenure-Track Recruiting Committee Member, 2020-21, 2021-22
- Graduate Study Committee Member, 2019-20, 2020-21, 2022-23, 2023-24