Dakshita Khurana

Email: dakshita@illinois.edu

WebURL: `https://www.dakshitakhurana.com/`

Research Interests: Cryptography, Theoretical Computer Science.

Employment

2019 – ... ◇ **University of Illinois Urbana-Champaign;**
Assistant Professor of Computer Science.

2018 – 19 ◇ **Microsoft Research, New England;**
Postdoctoral Researcher.

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.

Selected Honors

2023 ◇ **NSF CAREER Award:** Cryptographic Proofs, Outside the Black-Box.

◇ On the List of **Teachers Ranked as Excellent** for Spring 2023 at UIUC.

2022 ◇ **IIT Delhi Graduate of Last Decade (GOLD) Award.**

◇ **DARPA Forward Riser.**

◇ On the List of **Teachers Ranked as Excellent** for Fall 2022 at UIUC.

2021 ◇ **Visa Research Faculty Award.**

◇ Paper awarded **Long Plenary Talk** at Quantum Information Processing QIP'21.

◇ On the List of **Teachers Ranked as Excellent** for Spring 2021 at UIUC.

2020 ◇ On the List of **Forbes 30 under 30** in Science.

◇ **Google Research Fellow** at the Simons Institute, Berkeley.

2019 ◇ On the List of **Teachers Ranked as Excellent** for Fall 2019 at UIUC.

◇ Paper 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 ◇ Paper invited to the **SIAM J. Computing Special Issue** for FOCS 2017.

◇ **CISCO Outstanding Graduate** Student Research Award.

Publications

(Authors Alphabetical)

1. Bartusek, J. & Khurana, D. (2023). Cryptography with certified deletion. *Quantum Information Processing, QIP 2023. In Advances in Cryptology, CRYPTO 2023.*
2. Bartusek, J., Khurana, D. & Poremba, A. (2023). Publicly-verifiable deletion via target-collapsing functions. *In advances in cryptology, CRYPTO 2023.*
3. 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.*
4. Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2023b). Round-optimal black-box mpc in the plain model. *In Advances in Cryptology, CRYPTO 2023.*
5. Bartusek, J., Garg, S., Khurana, D. & Roberts, B. (2023). Blind delegation with certified deletion. *Quantum Information Processing, QIP 2023.*
6. Agarwal, A., Bartusek, J., Khurana, D. & Kumar, N. (2023). A new framework for quantum oblivious transfer. *In Advances in Cryptology - EUROCRYPT 2023.*
7. 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.*
8. Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2023a). Black-box reusable NISC with random oracles. *In Advances in Cryptology - EUROCRYPT 2023.*
9. Canetti, R., Chakraborty, S., Khurana, D., Kumar, N., Poburinnaya, O. & Prabhakaran, M. (2022). COA-secure obfuscation and applications. *In Advances in Cryptology, EUROCRYPT 2022.*
10. Hulett, J., Jawale, R., Khurana, D. & Srinivasan, A. (2022). SNARGS for P from sub-exponential DDH and QR. *In Advances in Cryptography, EUROCRYPT 2022.*
11. Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2022a). Round optimal black-box protocol compilers. *In Advances in Cryptology, EUROCRYPT 2022.*
12. 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.*
13. 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.*
14. 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.*
15. 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.**

16. 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.*

17. 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.*

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

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

20. 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.*

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

22. 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.*

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

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

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

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

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

28. Bitansky, N., Khurana, D. & Paneth, O. (2020). 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.**

29. Kalai, Y. T. & Khurana, D. (2018). Non-interactive non-malleability from quantum supremacy. *In Advances in Cryptology, CRYPTO 2019.*

30. 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.*

31. 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.*

32. Kalai, Y., Khurana, D. & Sahai, A. (2018). Statistical WI (and more) in 2 messages. *In Advances in Cryptology, EUROCRYPT 2018.*

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

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

35. 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 SIAM Journal on Computing (SICOMP) Special Issue for FOCS 2017.**

36. 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*.

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

38. 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*.

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

40. 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*.

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

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

43. 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*.

44. 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*.

45. 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*.

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

47. 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 Workshop on Cryptography from Minimal Assumptions;** *May 2023.*
2. Cryptography with Certified Deletion. **CMU Cylab Cryptography Seminar;** *Nov 2022.*
3. Quantum Cryptography from Minimal Assumptions. **Invited Tutorial at the UCLA IPAM Graduate Summer School on Post-quantum and Quantum Cryptography;** *July 2022.*
4. From Deletion to Secure Computation and Back. **Spotlight Talk at the Information Theoretic Cryptography Conference, Boston;** *July 2022.*
5. SNARGs and PPAD Hardness from Sub-exponential DDH and QR. **Boston Crypto Day;** *July 2022.*
6. Quantum Oblivious Transfer from One-way Functions. **Invited Talk at QCrypt;** *Aug 2021.*
7. On Removing Interaction in Non-Malleable Commitments. **MIT Cryptography and Information Security (CIS) Seminar;** *Apr 2021.*
8. Secure Federated Learning for Clinical Diagnostics with Applications to the COVID-19 Pandemic. **C3.AI DTI Virtual Symposium;** *Jan 2021.*
9. SNARGs and PPAD Hardness from Sub-exponential LWE. **TIFR School of Technology and Computer Science Colloquium;** *Dec 2020.*
10. Secure Federated Learning for Clinical Diagnostics. **Arches COVID Seminar;** *Nov 2020.*
11. Post-quantum Multi-party Computation. **Theory and Practice of Multiparty Computation Workshop (TPMPC) at Aarhus University;** *May 2020.*
12. New Techniques in Zero-Knowledge. **Trends in TCS Workshop, TTI Chicago;** *Jan 2020.*
13. Two-Message Statistically Private Arguments. **Simons Institue Workshop on Probabilistically Checkable and Interactive Proofs;** *Sep 2019.*
14. Weak Zero-Knowledge Beyond the Black-Box Barrier. **Carnegie Mellon University Theory talk;** *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,India;** *Dec 2018.*
17. Breaking Simulation Barriers. **University of Illinois Urbana-Champaign;** *Apr 2018.*

18. On Cryptographic Proof Systems. **Caltech CMS Theory Seminar;** *Dec 2017.*
19. New Techniques for Extraction. **South California Theory Day;** *Nov 2017.*
20. The Virtues of Two-Message OT. **Boston University Crypto Seminar;** *Sep 2017.*
21. Distinguisher-Dependent Simulation. **DIMACS Workshop on Outsourcing Computation Securely, Rutgers;** *Jul 2017.*
22. How to Achieve Non-Malleability in One or Two Rounds. **MIT Cryptography and Information Security (CIS) Seminar;** *Jun 2017.*
23. Birthday Simulation from Exponential Hardness, and its Applications. **New York Crypto Day at Cornell Tech;** *May 2017.*
24. Two-Message Non-Malleable Commitments. **UCSD Theory Seminar;** *Nov 2016.*
25. How to Generate and Use Universal Samplers. **Stanford DIMACS Workshop on Cryptography and Software Obfuscation;** *Nov 2016.*
26. Breaking the Three Round Barrier for Non-Malleable Commitments. **SIMONS Berkeley Cryptography Reunion Workshop;** *Aug 2016.*
27. Breaking the Three Round Barrier for Non-Malleable Commitments. **DIMACS Workshop on Cryptography and its Interactions, Rutgers;** *Jul 2016.*
28. How to Obtain Two-Message Non-Malleable Commitments. **MIT Cryptography and Information Security (CIS) Seminar;** *Jun 2016.*
29. Constructing Two-Message Non-Malleable Commitments. **New York University Cryptography Reading Group;** *May 2016.*
30. New Constructions of Non-Malleable Commitments. **Cornell Tech Cryptography Seminar;** *May 2016.*
31. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **Stanford Security Seminar;** *Feb 2016.*
32. How to Generate and Use Universal Samplers. **South California Theory Day, University of South California;** *Nov 2015.*
33. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **SIMONS Berkeley Workshop on Securing Computation;** *Aug 2015.*

Teaching

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

Teaching (continued)

- Fall 2022 ◇ Instructor, UIUC. Cryptography (Undergraduate) CS 407.
  Listed among Teachers Ranked as Excellent by Their Students.
- Spring 2022 ◇ Instructor, UIUC. Quantum Cryptography (Graduate) CS 598CTO.
- Fall 2021 ◇ Instructor, UIUC. Algorithms and Models of Computation (Undergraduate) CS 374.
- Spring 2021 ◇ Instructor, UIUC. Special Topics in Cryptography (Graduate) CS 598 DK.
  Listed among Teachers Ranked as Excellent by Their Students.
- Fall 2020 ◇ Instructor, UIUC. Applied Cryptography (Undergraduate) CS/ECE 498 AC (407).
- Fall 2019 ◇ Instructor, UIUC. Special Topics in Cryptography (Graduate) CS 598 DK.
  Listed among Teachers Ranked as Excellent by Their Students.

Students Advised

- PhD ◇ Ruta Jawale, 2019-Present.
- ◇ Amit Agarwal, 2019-Present.
- ◇ James Hulett, 2020-Present.
- ◇ Kabir Tomer, 2022-Present.
- MS ◇ Andrew Liu, 2020-21. *Secure and Scalable Robust Federated Learning.*
- ◇ Nishant Kumar, 2020-22. *New Frameworks for Quantum Oblivious Transfer.*

Current and Prior Research Support

- 2023-26 ◇ **NSF SaTC Small:** "New Cryptographic Capabilities for a Quantum World"
  PI: D.K. *USD 571,719.*
- 2023-28 ◇ **NSF CAREER:** "Cryptographic Proofs, Outside the Black-Box"
  PI: D.K. *USD 538,923.*
- 2021-23 ◇ **Visa Research Faculty Award**
  PI: D.K. *USD 150,000.*
- 2021-24 ◇ **NSF MPS/Physics**, "Pushing the Boundaries of Classical and Quantum Information Processing Toward Enhanced Security and Energy-Efficient Reliability".
  PI: E. Chitambar, co-PIs: L. Varshney, D.K. *USD 599,912.*
- 2020-24 ◇ **DARPA** "SIEVE: New Directions in Post-Quantum Zero-Knowledge".
  PI: Amit Sahai, co-PI: D.K. *UIUC subaward: USD 423,422.*
- 2019-21 ◇ **C3AI DTI, Jump Arches**, "Secure Federated Learning for Clinical Informatics".
  PI: O. Koyejo, co-PIs: W. Bond, D.K. *USD 100,000.*
- 2019-20 ◇ **Jump ARCHES**, "Secure Federated Learning for Clinical Diagnostics".
  PI: O. Koyejo, co-PIs: W. Bond, D.K. *USD 60,000.*

Service

Workshops

- Organizer of the Midwest Crypto Day, 2023- Present
- Co-organizer of the STOC'22 workshop: "The Multiple Facets of Quantum Proofs"
- PC co-chair of the Asiacrypt'22 Satellite workshop on Quantum Cryptography

PC Member

- STOC 2024
- ITCS 2023
- STOC 2022
- TCC 2022
- ACM India Doctoral Dissertation Award Committee 2022
- STOC 2020
- TCC 2020
- ITCS 2020
- Indocrypt 2020
- Eurocrypt 2019

UIUC Engg

- IQUIST (Illinois Quantum Information Science & Technology) Center. Science Advisory Board (SAB) Member, 2021-Present
- IDEA (Inclusion, Diversity, Equity and Access) Institute. Affiliate, 2020-Present

UIUC CS

- Broadening Participation in Computing Committee Member, 2021-22, 2022-23
- Tenure-Track Recruiting Committee Member, 2020-21, 2021-22
- Graduate Study Committee Member, 2019-20, 2020-21, 2022-23
- Rising Stars Workshop Mentor, 2019-20, 2020-21