

# Dakshita Khurana

Office: 4308 Siebel Center

Email: dakshita@illinois.edu

WebURL: <http://www.dakshitakhurana.com/>

**Research Interests:** Cryptography, broadly Theoretical Computer Science and Security.

## Employment

---

- 2019 -Present     ◇ **University of Illinois Urbana-Champaign.** Assistant Professor.
- 2018 -19     ◇ **Microsoft Research, New England.** Postdoctoral Researcher.
- 2018 -19     ◇ **University of Illinois Urbana-Champaign.** Adjunct Asst Professor.
- Summer 2017    ◇ **Microsoft Research, New England.** Research intern.
- Summer 2016    ◇ **Microsoft Research, New England.** Research intern.

## Education

---

- 2014 – 18     ◇ **Ph.D. in Computer Science** at University of California, Los Angeles.  
Advisors: Prof. Amit Sahai and Prof. Rafail Ostrovsky.
- 2012 – 14     ◇ **M.S. in Computer Science** at University of California, Los Angeles.
- 2008 – 12     ◇ **B. Tech. in Electrical Engineering with Minor in Computer Science**  
at Indian Institute of Technology (IIT), Delhi.

## Selected Awards

---

- 2020     ◇ Forbes 30 under 30, Science category.
- Spring '20    ◇ Google Research Fellow at Simons Institute, Berkeley.
- Fall '19    ◇ Teachers Ranked as Excellent by their Students, UIUC.
- 2017 – 18     ◇ UCLA CS Outstanding Graduating PhD Student Award.
- ◇ Dissertation Year Fellowship, University of California Los Angeles.
- ◇ Symantec Outstanding Graduate Student Research Award.
- ◇ STOC 2019 and FOCS 2017 papers invited to the SICOMP Special Issue.
- ◇ Invited Participant at Rising Stars in EECS, hosted by Stanford.
- 2016 – 17     ◇ CISCO Outstanding Graduate Student Research Award.
- ◇ Heidelberg Laureate Forum Young Researcher.
- 2014 – 15     ◇ Invited Participant at Women in Theory, hosted by New York University.
- 2012 – 13     ◇ Computer Science Dept Fellowship, University of California Los Angeles.
- 2009 – 10     ◇ Summer Undergraduate Research Award, IIT Delhi.
- 2006 – 08     ◇ National Kishore Vaigyanik Protsahan Yojana (KVPY) fellowship.

## Conference Proceedings

1. Badrinarayanan, S., Fernando, R., Jain, A., Khurana, D. & Sahai, A. (2020). Statistical zap arguments. *In Advances in Cryptology, EUROCRYPT 2020*.
2. Garg, A., Kalai, Y. & Khurana, D. (2020). Computational extractors with negligible error in the crs model. *In Advances in Cryptology, EUROCRYPT 2020*.
3. Khurana, D. & Mughees, M. H. (2020). On statistical security in two-party computation. *In Theory of Cryptography Conference, TCC 2020*.
4. Bitansky, N., Khurana, D. & Paneth, O. (2020). Weak zero-knowledge beyond the black-box barrier. *In Symposium on the Theory of Computing, STOC 2019*. **Invited to SICOMP Special Issue for STOC 2019**.
5. Kalai, Y. T. & Khurana, D. (2018). Non-interactive non-malleability from quantum supremacy. *In Advances in Cryptology, CRYPTO 2019*.
6. 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*.
7. 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*.
8. Kalai, Y., Khurana, D. & Sahai, A. (2018). Statistical WI (and more) in 2 messages. *In Advances in Cryptology, EUROCRYPT 2018*.
9. Badrinarayanan, S., Khurana, D., Sahai, A. & Waters, B. (2018). Upgrading to functional encryption. *In Theory of Cryptography Conference, TCC 2018*.
10. Khurana, D., Ostrovsky, R. & Srinivasan, A. (2018). Round optimal black-box “Commit-and-Prove”. *In Theory of Cryptography Conference, TCC 2018*.
11. 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 SICOMP Special Issue for FOCS 2017**.
12. 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*.
13. Badrinarayanan, S., Khurana, D., Ostrovsky, R. & Visconti, I. (2017). Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs. *In Advances in Cryptology, EUROCRYPT 2017*.

14. 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*.
15. Khurana, D. (2017). Round optimal concurrent non-malleability from polynomial hardness. In *Theory of Cryptography Conference, TCC 2017*.
16. 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*.
17. Khurana, D., Kraschewski, D., Maji, H. K., Prabhakaran, M. & Sahai, A. (2016). All complete functionalities are reversible. In *Advances in Cryptology, EUROCRYPT 2016*.
18. Khurana, D., Maji, H. K. & Sahai, A. (2016). Secure computation from elastic noisy channels. In *Advances in Cryptology, EUROCRYPT 2016*.
19. 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*.
20. 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*.
21. 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*.
22. Khurana, D., Rao, V. & Sahai, A. (2015). Multi-party key exchange for unbounded parties from indistinguishability obfuscation. In *Advances in Cryptology, ASIACRYPT 2015*.
23. Khurana, D., Maji, H. K. & Sahai, A. (2014). Black-box separations for differentially private protocols. In *Advances in Cryptology, ASIACRYPT 2014*.

## Invited Talks

---

1. Postquantum Multi-party Computation. **Theory and Practice of Multiparty Computation Workshop (TPMPC); May 2020.**
2. New Techniques in Zero-Knowledge. **Trends in TCS Workshop, TTI Chicago; January 2020.**
3. Two-Message Statistically Private Arguments. **Simons Institute Workshop on Probabilistically Checkable and Interactive Proofs; September 2019.**
4. Weak Zero-Knowledge Beyond the Black-Box Barrier. **Carnegie Mellon**

**University Theory talk; June 2019.**

5. Quantum Advantage and Classical Cryptography. **Charles River Crypto Day at Northeastern University; May 2019.**
6. New Techniques to Overcome Barriers in Simulation. **Indian Institute of Technology Mumbai, India; December 2018.**
7. Breaking Simulation Barriers. **University of Illinois Urbana-Champaign; April 2018.**
8. On Cryptographic Proof Systems. **Caltech CMS Theory Seminar; Dec 2017.**
9. New Techniques for Extraction. **South California Theory Day; Nov 2017.**
10. The Virtues of Two-Message OT. **Boston University Crypto Seminar; Sep 2017.**
11. Distinguisher-Dependent Simulation. **DIMACS Workshop on Outsourcing Computation Securely, Rutgers; July 2017.**
12. How to Achieve Non-Malleability in One or Two Rounds. **MIT Cryptography and Information Security (CIS) Seminar; June 2017.**
13. Birthday Simulation from Exponential Hardness, and its Applications. **New York Crypto Day at Cornell Tech; May 2017.**
14. How to use the Birthday Paradox to Design Protocols. **Carnegie Mellon University Theory talk; March 2017.**
15. Two-Message Non-Malleable Commitments. **UCSD Theory Seminar; Nov 2016.**
16. How to Generate and Use Universal Samplers. **Stanford DIMACS Workshop on Cryptography and Software Obfuscation; Nov 2016.**
17. Breaking the Three Round Barrier for Non-Malleable Commitments. **SIMONS Berkeley Cryptography Reunion Workshop; Aug 2016.**
18. Breaking the Three Round Barrier for Non-Malleable Commitments. **DIMACS Workshop on Cryptography and its Interactions, Rutgers; July 2016.**
19. How to Obtain Two-Message Non-Malleable Commitments. **MIT Cryptography and Information Security (CIS) Seminar; June 2016.**
20. Constructing Two-Message Non-Malleable Commitments. **New York University Cryptography Reading Group; May 2016.**
21. New Constructions of Non-Malleable Commitments. **Cornell Tech Cryptography Seminar; May 2016.**
22. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **Stanford Security Seminar; Feb 2016.**

23. How to Generate and Use Universal Samplers. **South California Theory Day, University of South California; Nov 2015.**
24. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **SIMONS Berkeley Workshop on Securing Computation; Aug 2015.**

## Conference Talks

---

25. Non-Interactive Non-Malleability from Quantum Supremacy at **CRYPTO, Santa Barbara; Aug 2019.**
26. Round Optimal Black-Box “Commit-and-Prove” at **TCC, Goa, India; Nov 2018.**
27. Non-interactive Delegation for Low-Space Non-Deterministic Computation at **STOC, Los Angeles; June 2018.**
28. Round Optimal Concurrent Non-Malleability from Polynomial hardness at **TCC, Baltimore; Nov 2017.**
29. How to Achieve Non-malleability in One or Two Rounds at **FOCS, Berkeley; Oct 2017.**
30. Distinguisher-dependent Simulation in Two Rounds and its Applications at **CRYPTO, Santa Barbara; Aug 2017.**
31. Breaking the Three Round Barrier for Non-malleable Commitments at **FOCS, Dimacs/Rutgers; Oct 2016.**
32. All Complete Functionalities are Reversible at **EUROCRYPT, Austria; May 2016.**
33. Secure Computation from Elastic Channels at **EUROCRYPT, Austria; May 2016.**
34. Multi-party Key Exchange for Unbounded Parties from Obfuscation at **Asiacrypt, New Zealand; Dec 2015.**
35. Black-Box Separations for Differentially Private Protocols at **Asiacrypt, Taiwan; Dec 2014.**

## Teaching

---

- |             |  |
|-------------|--|
| Fall 2020   | ◇ Instructor, UIUC. Applied Cryptography CS/ECE 498 AC (407).  |
| Fall 2019   | ◇ Instructor, UIUC. Special Topics in Cryptography CS 598 DK. <i>Listed among Teachers Ranked as Excellent by Their Students in Fall 2019.</i> |
| Winter 2014 | ◇ Teaching Assistant, CS at UCLA. Formal Languages and Automata.   |

## Service

---

- Program Committees
  - ◇ STOC 2020
  - ◇ TCC 2020
  - ◇ Indocrypt 2020
  - ◇ ITCS 2020
  - ◇ Eurocrypt 2019
- University Committees
  - ◇ UIUC Graduate Study Committee, 2019-20, 2020-21
  - ◇ Rising Stars Workshop Mentor, 2019-20, 2020-21
- Graduate Service
  - ◇ UCLA Ph.D. Admissions Committee, 2015-17
  - ◇ UCLA Graduate Student Ambassador, 2015-17