

# Dakshita Khurana

**Email:** dakshita@illinois.edu

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

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

## 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.  
Advisors: Prof. Amit Sahai and Prof. Rafail Ostrovsky.
- 2014           ◇ **M.S. in Computer Science** at the University of California, Los Angeles.
- 2012           ◇ **B. Tech. in Electrical Engineering with Minor in Computer Science**  
at the Indian Institute of Technology (IIT) Delhi, India.

## Selected Honors

---

- 2021           ◇ **Invited Talk at QCrypt'21** on Quantum OT from One-way Functions.  
◇ **Long Plenary Talk award** at Quantum Information Processing QIP'21.  
◇ On the List of **Teachers Ranked as Excellent** in 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** in Fall 2019 at UIUC.  
◇ 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.**  
◇ Invited Participant at **Rising Stars** in EECS, hosted by Stanford.
- 2017           ◇ 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.**

## Grants and Research Awards

---

- 2021     ◇ **Visa Research Award.**  
PI: D.K.
- 2021-24   ◇ **NSF QIS**, “Pushing the Boundaries of Classical and Quantum Information Processing Toward Enhanced Security and Energy-Efficient Reliability”.  
PI: E. Chitambar. Co-PIs: D.K. and L. Varshney.
- 2020-24   ◇ **DARPA “SIEVE: New Directions in Post-Quantum Zero-Knowledge”.**  
PI: Amit Sahai. Co-PI: D.K.
- 2020-21   ◇ **C3AI DTI**, “Secure Federated Learning for Clinical Informatics”.  
PI: O. Koyejo. Co-PIs: D.K., G. Heintz, W. Bond, R. Foulger.
- 2019-20   ◇ **Jump ARCHES**, “Secure Federated Learning for Clinical Diagnostics”.  
PI: O. Koyejo. Co-PIs: D.K., G. Heintz, W. Bond, R. Foulger.

## Publications

---

(Authors Alphabetical)

1.     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.*
2.     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.*
3.     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.*
4.     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.*
5.     Ishai, Y., Khurana, D., Sahai, A. & Srinivasan, A. (2021). On the round complexity of black-box secure MPC. *In Advances in Cryptology, CRYPTO 2021.*
6.     Khurana, D. & Srinivasan, A. (2021). Improved computational extractors and their applications. *In Advances in Cryptology, CRYPTO 2021.*
7.     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.*
8.     Khurana, D. (2021). Non-interactive distributional indistinguishability (NIDI) and non-malleable commitments. *In Advances in Cryptography, EUROCRYPT 2021.*
9.     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.*

10. Agarwal, A., Bartusek, J., Goyal, V., Khurana, D. & Malavolta, G. (2021a). Post-quantum multi-party computation. *In Advances in Cryptography, EUROCRYPT 2021*.
11. Garg, R., Lu, G., Khurana, D. & Waters, B. (2021). Black-box non-interactive non-malleable commitments. *In Advances in Cryptography, EUROCRYPT 2021*.
12. Badrinarayanan, S., Fernando, R., Jain, A., Khurana, D. & Sahai, A. (2020). Statistical zap arguments. *In Advances in Cryptology, EUROCRYPT 2020*.
13. Garg, A., Kalai, Y. & Khurana, D. (2020). Computational extractors with negligible error in the crs model. *In Advances in Cryptology, EUROCRYPT 2020*.
14. Khurana, D. & Mughees, M. H. (2020). On statistical security in two-party computation. *In Theory of Cryptography Conference, TCC 2020*.
15. 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**.
16. Kalai, Y. T. & Khurana, D. (2018). Non-interactive non-malleability from quantum supremacy. *In Advances in Cryptology, CRYPTO 2019*.
17. 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*.
18. 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*.
19. Kalai, Y., Khurana, D. & Sahai, A. (2018). Statistical WI (and more) in 2 messages. *In Advances in Cryptology, EUROCRYPT 2018*.
20. Badrinarayanan, S., Khurana, D., Sahai, A. & Waters, B. (2018). Upgrading to functional encryption. *In Theory of Cryptography Conference, TCC 2018*.
21. Khurana, D., Ostrovsky, R. & Srinivasan, A. (2018). Round optimal black-box “Commit-and-Prove”. *In Theory of Cryptography Conference, TCC 2018*.
22. 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**.
23. 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*.
24. Badrinarayanan, S., Khurana, D., Ostrovsky, R. & Visconti, I. (2017). Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs. *In Advances in Cryptology, EUROCRYPT 2017*.

25. 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*.
26. Khurana, D. (2017). Round optimal concurrent non-malleability from polynomial hardness. In *Theory of Cryptography Conference, TCC 2017*.
27. 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*.
28. 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*.
29. Khurana, D., Kraschewski, D., Maji, H. K., Prabhakaran, M. & Sahai, A. (2016). All complete functionalities are reversible. In *Advances in Cryptology, EUROCRYPT 2016*.
30. Khurana, D., Maji, H. K. & Sahai, A. (2016). Secure computation from elastic noisy channels. In *Advances in Cryptology, EUROCRYPT 2016*.
31. 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*.
32. 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*.
33. 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*.
34. Khurana, D., Rao, V. & Sahai, A. (2015). Multi-party key exchange for unbounded parties from indistinguishability obfuscation. In *Advances in Cryptology, ASIACRYPT 2015*.
35. Khurana, D., Maji, H. K. & Sahai, A. (2014). Black-box separations for differentially private protocols. In *Advances in Cryptology, ASIACRYPT 2014*.

## Invited Talks

---

1. Quantum Oblivious Transfer from One-way Functions. **Invited Talk at QCrypt; Aug 2021.**
2. On Removing Interaction in Non-Malleable Commitments. **MIT Cryptography and Information Security (CIS) Seminar; Apr 2021.**
3. Secure Federated Learning for Clinical Diagnostics with Applications to the COVID-19 Pandemic. **C3.AI DTI Virtual Symposium; Jan 2021.**
4. SNARGs and PPAD Hardness from Sub-exponential LWE. **TIFR School of Technology and Computer Science Colloquium; Dec 2020.**
5. Secure Federated Learning for Clinical Diagnostics. **Arches COVID Seminar; Nov 2020.**

6. Post-quantum Multi-party Computation. **Theory and Practice of Multiparty Computation Workshop (TPMPC) at Aarhus University**; *May 2020*.
7. New Techniques in Zero-Knowledge. **Trends in TCS Workshop, TTI Chicago**; *Jan 2020*.
8. Two-Message Statistically Private Arguments. **Simons Institute Workshop on Probabilistically Checkable and Interactive Proofs**; *Sep 2019*.
9. Weak Zero-Knowledge Beyond the Black-Box Barrier. **Carnegie Mellon University Theory talk**; *Jun 2019*.
10. Quantum Advantage and Classical Cryptography. **Charles River Crypto Day at Northeastern University**; *May 2019*.
11. New Techniques to Overcome Barriers in Simulation. **Indian Institute of Technology Mumbai, India**; *Dec 2018*.
12. Breaking Simulation Barriers. **University of Illinois Urbana-Champaign**; *Apr 2018*.
13. On Cryptographic Proof Systems. **Caltech CMS Theory Seminar**; *Dec 2017*.
14. New Techniques for Extraction. **South California Theory Day**; *Nov 2017*.
15. The Virtues of Two-Message OT. **Boston University Crypto Seminar**; *Sep 2017*.
16. Distinguisher-Dependent Simulation. **DIMACS Workshop on Outsourcing Computation Securely, Rutgers**; *Jul 2017*.
17. How to Achieve Non-Malleability in One or Two Rounds. **MIT Cryptography and Information Security (CIS) Seminar**; *Jun 2017*.
18. Birthday Simulation from Exponential Hardness, and its Applications. **New York Crypto Day at Cornell Tech**; *May 2017*.
19. Two-Message Non-Malleable Commitments. **UCSD Theory Seminar**; *Nov 2016*.
20. How to Generate and Use Universal Samplers. **Stanford DIMACS Workshop on Cryptography and Software Obfuscation**; *Nov 2016*.
21. Breaking the Three Round Barrier for Non-Malleable Commitments. **SIMONS Berkeley Cryptography Reunion Workshop**; *Aug 2016*.
22. Breaking the Three Round Barrier for Non-Malleable Commitments. **DIMACS Workshop on Cryptography and its Interactions, Rutgers**; *Jul 2016*.
23. How to Obtain Two-Message Non-Malleable Commitments. **MIT Cryptography and Information Security (CIS) Seminar**; *Jun 2016*.
24. Constructing Two-Message Non-Malleable Commitments. **New York University Cryptography Reading Group**; *May 2016*.

25. New Constructions of Non-Malleable Commitments. **Cornell Tech Cryptography Seminar**; *May 2016*.
26. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **Stanford Security Seminar**; *Feb 2016*.
27. How to Generate and Use Universal Samplers. **South California Theory Day, University of South California**; *Nov 2015*.
28. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **SIMONS Berkeley Workshop on Securing Computation**; *Aug 2015*.

## Conference Talks

---

29. Non-Interactive Distributional Indistinguishability and Non-malleable Commitments at **EUROCRYPT**; *Oct 2021*.
30. Improved Computational Extractors and their Applications at **CRYPTO**; *Aug 2021*.
31. Computational Extractors with Negligible Error in the CRS Model at **EUROCRYPT**; *May 2020*.
32. Non-Interactive Non-Malleability from Quantum Supremacy at **CRYPTO**, *Aug 2019*.
33. Round Optimal Black-Box “Commit-and-Prove” at **TCC**, *Nov 2018*.
34. Non-interactive Delegation for Low-Space Non-Deterministic Computation at **STOC**, *June 2018*.
35. Round Optimal Concurrent Non-Malleability from Polynomial hardness at **TCC**, *Nov 2017*.
36. How to Achieve Non-malleability in One or Two Rounds at **FOCS**, *Oct 2017*.
37. Distinguisher-dependent Simulation in Two Rounds and its Applications at **CRYPTO**, *Aug 2017*.
38. Breaking the Three Round Barrier for Non-malleable Commitments at **FOCS**, *Oct 2016*.
39. All Complete Functionalities are Reversible at **EUROCRYPT** *May 2016*.
40. Secure Computation from Elastic Channels at **EUROCRYPT**, *May 2016*.
41. Multi-party Key Exchange for Unbounded Parties from Obfuscation at **Asiacrypt**, *Dec 2015*.
42. Black-Box Separations for Differentially Private Protocols at **Asiacrypt**, *Dec 2014*.

## Teaching

---

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

## Service

---

- Program Committee Member   ◇ STOC 2022
- ◇ TCC 2022
- ◇ STOC 2020
- ◇ TCC 2020
- ◇ ITCS 2020
- ◇ Eurocrypt 2019
- UIUC Committee Member   ◇ Broadening Participation in Computing Committee, 2021-22
- ◇ Tenure-Track Recruiting Committee, 2020-21
- ◇ Graduate Study Committee, 2019-20, 2020-21
- ◇ Rising Stars Workshop Mentor, 2019-20, 2020-21