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 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

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

2021 ◇ Plenary Talk at Quantum Information Processing QIP'21.

2020 ◇ Forbes 30 under 30, Science category.

◇ Google Research Fellow at Simons Institute, Berkeley.

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

◇ STOC'19 paper invited to the SICOMP Special Issue.

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 ◇ FOCS'17 paper invited to the SICOMP Special Issue.

◇ CISCO Outstanding Graduate Student Research Award.

◇ Invited as Young Researcher to the Heidelberg Laureate Forum.

2015 ◇ Invited Participant at Women in Theory, hosted by New York University.

2012 – 13 ◇ Computer Science Dept Fellowship, University of California Los Angeles.

Publications (Authors Alphabetical)

1. Bartusek, J., Coladangelo, A., Khurana, D. & Ma, F. (2021b). One-way functions imply secure computation in a quantum world. *In Quantum Information Processing, QIP 2021*. **Plenary Talk at QIP 2021.**

2. Bartusek, J., Coladangelo, A., Khurana, D. & Ma, F. (2021a). On the round complexity of two-party quantum computation. *In Quantum Information Processing, QIP 2021*.

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

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

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

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

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

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

9. 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.**

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

11. 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*.

12. 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*.

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

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

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

16. 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.**

17. 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*.

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

19. 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*.

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

21. 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*.

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

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

24. 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*.

25. 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*.

26. 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*.

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

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

Invited Talks

1. Secure Federated Learning for Clinical Diagnostics with Applications to the COVID-19 Pandemic. **C3.AI DTI Virtual Symposium;** *January 2021*.
2. SNARGs and PPAD Hardness from Sub-exponential LWE. **TIFR School of Technology and Computer Science Colloquium;** *December 2020*.
3. Secure Federated Learning for Clinical Diagnostics. **Arches COVID Seminar;** *November 2020*.
4. Post-quantum Multi-party Computation. **Theory and Practice of Multiparty Computation Workshop (TPMPC) at Aarhus University;** *May 2020*.
5. New Techniques in Zero-Knowledge. **Trends in TCS Workshop, TTI Chicago;** *January 2020*.
6. Two-Message Statistically Private Arguments. **Simons Institue Workshop on Probabilistically Checkable and Interactive Proofs;** *September 2019*.
7. Weak Zero-Knowledge Beyond the Black-Box Barrier. **Carnegie Mellon University Theory talk;** *June 2019*.
8. Quantum Advantage and Classical Cryptography. **Charles River Crypto Day at Northeastern University;** *May 2019*.
9. New Techniques to Overcome Barriers in Simulation. **Indian Institute of Technology Mumbai, India;** *December 2018*.
10. Breaking Simulation Barriers. **University of Illinois Urbana-Champaign;** *April 2018*.
11. On Cryptographic Proof Systems. **Caltech CMS Theory Seminar;** *Dec 2017*.
12. New Techniques for Extraction. **South California Theory Day;** *Nov 2017*.
13. The Virtues of Two-Message OT. **Boston University Crypto Seminar;** *Sep 2017*.
14. Distinguisher-Dependent Simulation. **DIMACS Workshop on Outsourcing Computation Securely, Rutgers;** *July 2017*.
15. How to Achieve Non-Malleability in One or Two Rounds. **MIT Cryptography and Information Security (CIS) Seminar;** *June 2017*.
16. Birthday Simulation from Exponential Hardness, and its Applications. **New York Crypto Day at Cornell Tech;** *May 2017*.

17. How to use the Birthday Paradox to Design Protocols. **Carnegie Mellon University Theory talk;** *March 2017.*

18. Two-Message Non-Malleable Commitments. **UCSD Theory Seminar;** *Nov 2016.*

19. How to Generate and Use Universal Samplers. **Stanford DIMACS Workshop on Cryptography and Software Obfuscation;** *Nov 2016.*

20. Breaking the Three Round Barrier for Non-Malleable Commitments. **SIMONS Berkeley Cryptography Reunion Workshop;** *Aug 2016.*

21. Breaking the Three Round Barrier for Non-Malleable Commitments. **DIMACS Workshop on Cryptography and its Interactions, Rutgers;** *July 2016.*

22. How to Obtain Two-Message Non-Malleable Commitments. **MIT Cryptography and Information Security (CIS) Seminar;** *June 2016.*

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

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

25. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **Stanford Security Seminar;** *Feb 2016.*

26. How to Generate and Use Universal Samplers. **South California Theory Day, University of South California;** *Nov 2015.*

27. Multi-party Key Exchange for Unbounded Parties from Obfuscation. **SIMONS Berkeley Workshop on Securing Computation;** *Aug 2015.*

Conference Talks

28. Non-Interactive Non-Malleability from Quantum Supermacy at **CRYPTO, Santa Barbara;** *Aug 2019.*

29. Round Optimal Black-Box "Commit-and-Prove" at **TCC, Goa, India;** *Nov 2018.*

30. Non-interactive Delegation for Low-Space Non-Deterministic Computation at **STOC, Los Angeles;** *June 2018.*

31. Round Optimal Concurrent Non-Malleability from Polynomial hardness at **TCC, Baltimore;** *Nov 2017.*

32. How to Achieve Non-malleability in One or Two Rounds at **FOCS, Berkeley;** *Oct 2017.*

33. Distinguisher-dependent Simulation in Two Rounds and its Applications at

CRYPTO, Santa Barbara; *Aug 2017.*

34. Breaking the Three Round Barrier for Non-malleable Commitments at **FOCS, Dimacs/Rutgers;** *Oct 2016.*

35. All Complete Functionalities are Reversible at **EUROCRYPT, Austria;** *May 2016.*

36. Secure Computation from Elastic Channels at **EUROCRYPT, Austria;** *May 2016.*

37. Multi-party Key Exchange for Unbounded Parties from Obfuscation at **Asiacrypt, New Zealand;** *Dec 2015.*

38. Black-Box Separations for Differentially Private Protocols at **Asiacrypt, Taiwan;** *Dec 2014.*

Teaching

Spring 2021 ◇ Instructor, UIUC. Special Topics in Cryptography CS 598 DK.

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 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

Other Service
- ◇ UCLA Ph.D. Admissions Committee, 2015-17
- ◇ UCLA Graduate Student Ambassador, 2015-17