

Curriculum Vitae

Mohammad Mahmoody

March 1, 2023

www.cs.virginia.edu/~mohammad/
mohammad@virginia.edu
Google Scholar

Address: PO Box 400740
85 Engineer's Way
Charlottesville, VA, USA

Contents

Interests	1
Positions	1
Education	2
Honors	2
Mentorship	2
Publication	3
Grants	8
Service	8
Talks	9

Interests

I am interested in theoretical aspects of cryptography and their interplay with computational complexity. I am also interested in theoretical aspects of machine learning. I am primarily interested in understanding the inherent barriers, also known as lower bounds, impossibilities, or separations.

Positions

- **University of Virginia**, Charlottesville, USA.
Associate Professor (with Tenure) in Computer Science, Aug 2019–present.
- **University of California**, Berkeley, USA.
Visiting Research Engineer, July 2019–Aug 2020.
- **University of Virginia**, Charlottesville, USA.
Assistant Professor in Computer Science, Aug 2013–Aug 2019.

Education

- **Cornell University**, Ithaca, USA.
Postdoctoral Research Associate, Advisor: Rafael Pass, 2010–2013.
- **Princeton University**, Princeton, USA.
Ph.D. in Computer Science, Major: Theory, Advisor: Boaz Barak, 2005–2010.
- **Sharif University of Technology**, Tehran, Iran.
B.Sc. in Computer Engineering, Major: Software Engineering, 2000–2004.

Honors

- University of Virginia’s School of Engineering & Applied Science Research Innovation Awards, 2017, 2018 (lead PI), and 2019.
- NSF CAREER award, 2014.
- The Gordon Wu Prize for Excellence, Princeton University, 2009.
- First Rank, National Graduate Entrance Exam in Computer Science, Iran, 2004.
- Gold Medal, National Olympiad in Informatics, Iran, 1999.

Mentorship

- **Graduate Students.** For graduate students, the graduating year is mentioned, followed by the first job or the hosting school.
 - Abtin Afshar, PhD, ongoing.
 - Wei Qi, Masters 2022 → PhD, ongoing.
 - Ji Gao, PhD, 2022 → Meta.
 - Saeed Mahloujifar, PhD, 2020 → Postdoc at Princeton.
 - Ameer Mohammed, PhD, 2018 → Assistant Professor at Kuwait University.
 - Ahmadreza Rahimi, Masters, 2020 → PhD at Max Planck Institute.
 - Caleb Smith, Masters, 2020 → DZYNE Technologies.
 - Saba Eskandarian, Masters, 2016 → PhD at Stanford.
 - Soheil Nematihaji, Masters, 2016 → InMoment.
 - Elahe Sadeghi, Graduate Student 09/2021–09/2022 → PhD at UT Austin.
- **Postdocs**
 - Mohammad Hajiabadi, Jan 2018–June 2018, (jointly advised with Sanjam Garg) → Assistant Professor at PSU → Assistant Professor at Waterloo.
 - Dimitris I. Diochnos, June 2018–June 2019 → Assistant Professor at The University of Oklahoma.

Publication

In theoretical computer science, the custom is that the authors' names appear in the alphabetical order. Most papers below follow this tradition. For other papers, a star "*" indicates equal (first-author level of) contribution. Names that are underlined indicate the author was a member of my group at the time. Links to the full versions are available on my academic homepage:

<http://www.cs.virginia.edu/~mohammad/>

Conference Papers

49. Abtin Afshar, Geoffroy Couteau, Mohammad Mahmoody, and Elahe Sadeghi. *Fine-Grained Non-Interactive Key-Exchange: Constructions and Lower Bounds*. Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2023.
48. Kai-Min Chung, Yao-Ting Lin, and Mohammad Mahmoody. *Black-Box Separations for Non-Interactive Commitments in a Quantum World*. A Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2023.
47. Steve Hanneke, Amin Karbasi, Mohammad Mahmoody, Idan Mehalal, and Shay Moran. *On Optimal Learning Under Targeted Data Poisoning*. Conference on Neural Information Processing Systems (NeurIPS) 2022 (*selected for oral presentation*).
46. Sanjam Garg, Somesh Jha, Saeed Mahloujifar, Mohammad Mahmoody, and Mingyuan Wang. *Overparameterization from Computational Constraints*. Conference on Neural Information Processing Systems (NeurIPS) 2022.
45. Mohammad Mahmoody, Wei Qi, and Ahmadreza Rahimi. *Lower Bounds for the Number of Decryption Updates in Registration-Based Encryption*. (To appear in) Theory of Cryptography Conference (TCC) 2022.
44. Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, and Mohammad Mahmoody. *On the Impossibility of Key Agreements from Quantum Random Oracles*. International Cryptology Conference (CRYPTO) 2022.
43. Ji Gao, Sanjam Garg, Mohammad Mahmoody, and Prashant Vasudevan. *Deletion Inference, Reconstruction, and Compliance in Machine (Un)Learning*. Privacy Enhancing Technologies Symposium (PETS) 2022.
42. Sanjam Garg, Somesh Jha, Saeed Mahloujifar, Mohammad Mahmoody, and Abhradeep Thakurta. *A Separation Result Between Data-oblivious and Data-aware Poisoning Attacks*. Conference on Neural Information Processing Systems (NeurIPS) 2021.
41. Omid Etesami, Ji Gao, Saeed Mahloujifar, and Mohammad Mahmoody. *Polynomial-time targeted attacks on coin tossing for any number of corruptions*. Theory of Cryptography Conference (TCC) 2021.
40. Ji Gao, Amin Karbasi, and Mohammad Mahmoody. *Learning and certification under instance-targeted poisoning*. The Conference on Uncertainty in Artificial Intelligence (UAI) 2021.

39. Nicholas Carlini, Samuel Deng, Sanjam Garg, Somesh Jha, Saeed Mahloujifar, Mohammad Mahmoody, Shuang Song, Abhradeep Thakurta, and Florian Tramer. *Is Private Learning Possible with Instance Encoding?* IEEE Symposium on Security & Privacy (Oakland) 2021.
38. Geoffroy Couteau, Pooya Farshim, and Mohammad Mahmoody. *Black-Box Uselessness: Composing Separations in Cryptography*. Proceedings of the 12th Conference on Innovations in Theoretical Computer Science (ITCS) 2021.
37. Dimitrios I. Diochnos*, Saeed Mahloujifar*, and Mohammad Mahmoody. *Lower Bounds for Adversarially Robust PAC Learning under Evasion and Hybrid Attacks*. IEEE International Conference On Machine Learning and Applications (ICMLA) 2020.
36. Mohammad Mahmoody, [Caleb Smith](#), and David J. Wu. *Can Verifiable Delay Functions be Based on Random Oracles?* International Colloquium on Automata, Languages and Programming (ICALP) 2020.
35. Sanjam Garg, Somesh Jha, [Saeed Mahloujifar](#), and Mohammad Mahmoody. *Adversarially Robust Learning Could Leverage Computational Hardness*. Algorithmic Learning Theory (ALT) 2020.
34. Omid Etesami, [Saeed Mahloujifar](#), and Mohammad Mahmoody. *Computational Concentration of Measure: Optimal Bounds, Reductions, and More*. ACM-SIAM Symposium on Discrete Algorithms (SODA) 2020.
33. [Saeed Mahloujifar*](#), [Xiao Zhang*](#), Mohammad Mahmoody, and David Evans. *Empirically Measuring Concentration: Fundamental Limits on Intrinsic Robustness*. Conference on Neural Information Processing Systems (NeurIPS) 2019 (*spotlight presentation*).
32. [Saeed Mahloujifar](#), Mohammad Mahmoody, and [Ameer Mohammed](#). *Universal Multi-party Poisoning Attacks*. International Conference on Machine Learning (ICML) 2019.
31. Sanjam Garg, [Mohammad Hajiabadi](#), Mohammad Mahmoody, [Ahmadreza Rahimi](#), and Sruthi Sekar. *Registration-Based Encryption from Standard Assumptions*. International Conference on Practice and Theory of Public Key Cryptography (PKC) 2019.
30. [Saeed Mahloujifar](#) and Mohammad Mahmoody. *Can Adversarially Robust Learning Leverage Computational Hardness?* Algorithmic Learning Theory (ALT) 2019.
29. [Saeed Mahloujifar](#), [Dimitrios I. Diochnos](#), and Mohammad Mahmoody. *The Curse of Concentration in Robust Learning: Evasion and Poisoning Attacks from Concentration of Measure*. AAAI conference on artificial intelligence, 2019.
28. Dimitrios I. Diochnos*, [Saeed Mahloujifar*](#), and Mohammad Mahmoody. *Adversarial Risk and Robustness: General Definitions and Implications for the Uniform Distribution*. Conference on Neural Information Processing Systems (NeurIPS) 2018.
27. Sanjam Garg, [Mohammad Hajiabadi](#), Mohammad Mahmoody, and [Ahmadreza Rahimi](#). *Registration-Based Encryption: Removing Private-Key Generator from IBE*. Theory of Cryptography Conference (TCC) 2018.

26. Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, and Ameer Mohammed. *Limits on the Power of Garbling Techniques for Public-Key Encryption*. Annual International Cryptology Conference (CRYPTO) 2018.
25. Sanjam Garg, Mohammad Mahmoody, Daniel Masny, and Izaak Meckler. *On the Round Complexity of OT Extension*. Annual International Cryptology Conference (CRYPTO) 2018.
24. Saeed Mahloujifar, Dimitrios I. Diochnos, and Mohammad Mahmoody. *Learning under p -Tampering Attacks*. Algorithmic Learning Theory (ALT) 2018.
23. Mohammad Mahmoody and Saeed Mahloujifar. *Blockwise p -Tampering Attacks on Cryptographic Primitives, Extractors, and Learners*. Theory of Cryptography Conference (TCC) Springer, Cham, pp. 245–279, 2017.
22. Sanjam Garg and Mohammad Mahmoody and Ameer Mohammad. *When Does Functional Encryption Imply Obfuscation?* Theory of Cryptography Conference (TCC) Springer, Cham, pp. 82–115, 2017.
21. Sanjam Garg and Mohammad Mahmoody and Ameer Mohammad. *Lower Bounds on Indistinguishability Obfuscation from All-or-Nothing Encryption Primitives*. Annual International Cryptology Conference (CRYPTO) Springer, Cham, pp. 661–695, 2017
20. Mohammad Mahmoody and Ameer Mohammed. *On the Power of Hierarchical Identity-Based Encryption*. Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt) Springer, Berlin, Heidelberg, 243–272, 2016.
19. Mohammad Mahmoody, Ameer Mohammed, and Soheil Nematihaji. *On the Impossibility of Virtual Black-Box Obfuscation in Idealized Models*. Theory of Cryptography Conference (TCC) Springer, Berlin, Heidelberg, pp. 18–48, 2016.
18. Mohammad Mahmoody, Ameer Mohammed, Soheil Nematihaji, Rafael Pass, and abhi shelat. *Lower Bounds on Assumptions behind Indistinguishability Obfuscation*. Theory of Cryptography Conference (TCC) Springer, Berlin, Heidelberg, pp. 49–66, 2016.
17. Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth. *On the Impossibility of Cryptography with Tamperable Randomness*. International Cryptology Conference (CRYPTO) Springer, Berlin, Heidelberg, pp. 462–479, 2014.
Invited to the Journal Algorithmica.
16. Dana Dachman-Soled, Mohammad Mahmoody, and Tal Malkin. *Can Optimally-Fair Coin Tossing be Based on One-Way Functions?* Theory of Cryptography Conference (TCC) Springer, Berlin, Heidelberg, pp. 217–239, 2014.
15. Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. *On the Power of Public-key Encryption in Secure Computation*. Theory of Cryptography Conference (TCC) Springer, Berlin, Heidelberg, pp. 240–264, 2014.
14. Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. *Limits of Random Oracles in Secure Computation*. Proceedings of the 5th Conference on Innovations in Theoretical Computer Science (ITCS) ACM, pp. 23–34, 2014.

13. Mohammad Mahmoody and David Xiao. *Languages with Efficient Zero Knowledge PCPs are in SZK*. Theory of Cryptography Conference (TCC) Springer, pp. 297–314, 2013.
Invited to TCC's special issue in Computational Complexity Journal.
12. Kai-Min Chung, Huijia Lin, Mohammad Mahmoody, and Rafael Pass. *On the Power of Nonuniformity in Proofs of Security*. Proceedings of the 4th Conference on Innovations in Theoretical Computer Science (ITCS) ACM, pp. 389–400, 2013.
11. Mohammad Mahmoody, Tal Moran and Salil Vadhan. *Publicly Verifiable Proofs of Sequential Work*. Proceedings of the 4th Conference on Innovations in Theoretical Computer Science (ITCS) ACM, pp. 373–388, 2013.
10. Mohammad Mahmoody and Rafael Pass. *The curious case of non-interactive commitments—on the power of black-box vs. non-black-box use of primitives*. Advances in Cryptology (CRYPTO) Springer, Berlin, Heidelberg, pp. 701–718, 2012.
9. Yuval Ishai, Mohammad Mahmoody, and Amit Sahai. *On Efficient Zero-Knowledge PCPs*. Theory of Cryptography Conference (TCC) Springer, Berlin, Heidelberg, pp. 151–168, 2012.
Invited to the Journal of Cryptology.
8. Vipul Goyal, Virendra Kumar, Satya Lokam, and Mohammad Mahmoody. *On Black-Box Reductions between Predicate Encryption Schemes*. Theory of Cryptography Conference (TCC) Springer, Berlin, Heidelberg, pp. 440–457, 2012.
7. Mohammad Mahmoody, Tal Moran, and Salil Vadhan. *Time-Lock Puzzles in the Random Oracle Model*. Annual Cryptology Conference (CRYPTO) Springer, pp. 39–50, 2011.
6. Dana Dachman-Soled, Yehuda Lindell, Mohammad Mahmoody, and Tal Malkin. *On the Black-Box Complexity of Optimally-Fair Coin Tossing*. Theory of Cryptography Conference (TCC) Springer, Berlin, Heidelberg, pp. 450–467, Springer, 2011.
5. Vipul Goyal, Yuval Ishai, Mohammad Mahmoody, and Amit Sahai. *Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography*. Annual Cryptology Conference (CRYPTO) Springer, Berlin, Heidelberg, pp. 173–190, 2010.
4. Mohammad Mahmoody and David Xiao. *On the Power of Randomized Reductions and the Checkability of SAT*. 25th Annual Conference on Computational Complexity (CCC) IEEE, pp. 64–75, 2010.
3. Iftach Haitner, Mohammad Mahmoody, and David Xiao. *A New Sampling Protocol and Applications to Basing Cryptographic Primitives on Hardness of NP*. 25th Annual Conference on Computational Complexity (CCC) IEEE, 76–87, 2010.
2. Boaz Barak and Mohammad Mahmoody. *Merkle Puzzles are Optimal: An $O(n^2)$ Attack on any Key Agreement from Random Oracles*. Advances in Cryptology (CRYPTO) Springer, Berlin, Heidelberg, 374–390, 2009. ***Invited to the Journal of Cryptology.***
1. Boaz Barak and Mohammad Mahmoody. *Lower Bounds on Signatures from Symmetric Primitives*. 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS) IEEE, 680–688, 2007.

Journal Papers

6. Saeed Mahloujifar, Dimitrios I. Diochnos, and Mohammad Mahmoody. *Learning under p -Tampering Poisoning Attacks*. Annals of Mathematics and Artificial Intelligence, Vol. 88, pp. 759–792, 2020.
5. Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth. *On the Impossibility of Cryptography with Tamperable Randomness*. Algorithmica, Vol. 79.4, pp. 1052–1101, 2017.
4. Boaz Barak and Mohammad Mahmoody. *Merkle’s Key Agreement Protocol is Optimal: An $O(n^2)$ Attack on Any Key Agreement from Random Oracles*. Journal of Cryptology, Vol. 30.3, pp. 699–734, 2017.
3. Amir Nayyeri, Sajjad Zarifzadeh, Nasser Yazdani, and Mohammad Mahmoody. *Load sensitive topology control: Towards minimum energy consumption in dense ad hoc sensor networks*. J. of Computer Networks, Vol. 52, pp. 493–513, 2008.
2. Saieed Akbari, Omid Etesami, Hamid Mahini, Mohammad Mahmoody. *On Rainbow Cycles in Edge-Colored Complete Graphs*. Australasian Journal of Combinatorics, Vol. 37, pp. 33–42, 2007.
1. Saieed Akbari, Omid Etesami, Hamid Mahini, Mohammad Mahmoody, and Ali Sharifi. *Transversals in Long Rectangular Arrays*. Discrete Mathematics Journal, Vol. 306, pp. 3011–3013, 2006.

Manuscripts

- Nicholas Carlini, Sanjam Garg, Somesh Jha, Saeed Mahloujifar, Mohammad Mahmoody, and Florian Tramèr. *NeuraCrypt is not private*.
- Mohammad Etemad, Mohammad Mahmoody, and David Evans. *Optimizing Trees for Static Searchable Encryption*. Cryptology ePrint 2018/052.
- *Studies in the Efficiency and (versus) Security of Cryptographic Tasks*. Mohammad Mahmoody. Ph.D Thesis, Princeton University, 2010.
- *Black Boxes, Incorporated*. (a survey) Mohammad Mahmoody and Avi Wigderson.
- *A Note on Black-Box Separations for Indistinguishability Obfuscation*. Mohammad Mahmoody, Ameer Mohammed, Soheil Nematihaji, Rafael Pass, and abhi shelat. Cryptology ePrint Archive, Report 2016/316.
- *Unprovable Security of 2-Message Zero-Knowledge*. Kai-Min Chung, Edward Lui, Mohammad Mahmoody, and Rafael Pass. Cryptology ePrint report 2012/711.

Grants

- NSF Medium, CNS-1936799, *New Directions in Public-Key and Identity-Based Encryption*, PIs: Sanjam Garg (UC Berkeley, PI), Mohammad Mahmoody (UVa, co-PI), 12/1/2019–11/30/2023, total award amount: \$1,097,000; UVa’s award amount: \$497,224.
- NSF Small, CCF-1910681, *Barriers in Adversarially Robust Learning*, 10/1/2019–09/30/2022, award amount: \$400,000.
- Supplement 8/1/2017–7/31/2018 for PI: Sanjam Garg (UC Berkeley) with supplement’s total: \$190,000. UVa’s amount: \$110,000 awarded as subcontract #00009696 from Berkeley.
- NSF CAREER, CCF-1350939, *Separations in Cryptography*, 06/01/2014–05/31/2019, award amount: \$423,000.
- University of Virginia’s School of Engineering & Applied Science Innovation Awards:
 - *Privacy-preserving machine learning via robust learning and noisy computation*, together with David Evans, Yuan Tian, and (the lead PI) David Wu (2019–2020).
 - *Revisiting Algorithmic Fairness and its Robustness in Adversarial Settings*, as the lead PI, together with Peter Beling, David Evans, and Hongning Wang (2018–2019).
 - *Machine Learning in Adversarial Contexts*, together with Homa Alemzadeh, (the lead PI) David Evans, Yanjun Qi, and Quanquan Gu (2017–2018).

Service

- **Conference Program Committees**
 - International Conference on Machine Learning (ICML) 2023.
 - Theory of Cryptography Conference (TCC) 2023.
 - International Conference on Learning Representations (ICLR) 2023.
 - Conference on Neural Information Processing Systems (NeurIPS) 2022.
 - Theory of Cryptography Conference (TCC) 2022.
 - International Cryptology Conference (CRYPTO) 2022.
 - International Conference on Machine Learning (ICML) 2022.
 - Conference on Information-Theoretic Cryptography (ITC) 2022.
 - International Conference on Learning Representations (ICLR) 2022.
 - The 3rd Privacy-Preserving Machine Learning Workshop, CRYPTO Affiliated Event, 2021. (Contributed talks committee member.)
 - Conference on Neural Information Processing Systems (NeurIPS) 2021.
 - Conference on Information-Theoretic Cryptography (ITC) 2021.
 - International Conference on Learning Representations (ICLR) 2021. ***Outstanding reviewer award.***

- Theory of Cryptography Conference (TCC) 2020.
- Conference on Neural Information Processing Systems (NeurIPS) 2020.
- International Cryptology Conference (CRYPTO) 2020.
- Topics in Theoretical Computer Science (TTCS) 2020.
- Theory of Cryptography Conference (TCC) 2019.
- Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2019.
- Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2018.
- ACM Conference on Computer and Communications Security (CCS) 2017.
- International Cryptology Conference (CRYPTO) 2017.
- Topics in Theoretical Computer Science (TTCS) 2017.
- Theory of Cryptography Conference (TCC) 2015.
- Topics in Theoretical Computer Science (TTCS) 2015.
- Theory of Cryptography Conference (TCC) 2014.
- Theory of Cryptography Conference (TCC) 2013.
- Theory of Cryptography Conference (TCC) 2011.

- **Organized Workshops**

- Organizing (together with Iftach Haitner, Yuval Ishai, Pooya Farschim) the workshop “Lower Bounds in Cryptography”, Bertinoro Italy, July 2019.
- Helped organize DC-area crypto days (Sept’14 – Sept’21).
- Helped organize Cyberwars workshop at UVA, A GenCyber Camp, June 2018.

- **Journal Refereeing**

- Theory of Computing, Journal of Cryptology, Transactions on Computing Theory, Random Structures and Algorithms, SIAM Journal on Computing (SICOMP), Cryptography and Communications, Computational Complexity Journal, Theoretical Computer Science, Journal of Computing and Security, Journal of the ACM, Journal of Information Security and Applications, Quantum Information Processing, Algorithmica.

Talks

- *On Privacy Implications of Machine Unlearning*. Invited speaker to Google’s virtual seminar on privacy, Google (virtual), June 2022.
- *Deletion Inference, Reconstruction, and Compliance in Machine (Un)Learning*. Invited speaker to the 56th Annual Conference on Information Sciences and Systems (CISS), Princeton (virtual), March 2022.
- *Connections between cryptographic coin flipping and adversarially robust learning*. Invited speaker at The 2nd Privacy-Preserving Machine Learning Workshop, Crypto (virtual) 2020.

- *On the (im)possibility of VDFs in the Random Oracle Mode.* Stanford's VDF day, Stanford, Feb 2020.
- *Computational concentration of measure.* Theory Lunch, Computer Science Department, UC Berkeley, Oct 2019.
- *Coin-tossing attacks, computational concentration of products, and limits of robust learning.* Theory Seminar, Computer Science Department, University of Washington, April 2019.
- *Registration-Based Encryption.* DC Area Crypto Day, National Institute of Standards and Technology (NIST), April 2019.
- *How far can robust classification go?* Human and Machine Intelligence Group, Humanities Informatics Lab, University of Virginia, March 2019.
- *Coin Tossing, Concentration of Products, and Limits of Robust Learning.* Charles River Crypto Day, MIT, March 2019.
- *Learning under p -Tampering Attacks.* DC-Area Anonymity, Privacy, and Security Seminar, George Mason University, February 2018.
- *Blockwise p -Tampering Attacks on Cryptographic Primitives, Extractors, and Learners.* Bay Area Crypto Day, Berkeley, November 2017.
- *Black-box and Non-black-box Lower Bounds on Assumptions behind Indistinguishability Obfuscation.* DIMACS Workshop on Complexity of Cryptographic Primitives and Assumptions, City College of New York, June 2017.
- *Lower bounds on Indistinguishability Obfuscation from All-or-Nothing Encryption.* Theory Seminar, Computer Science Department, Johns Hopkins University, March 2017.
- *Lower Bounds on IO from All-or-Nothing Encryption Primitives.* DIMACS/CEF Workshop on Cryptography and Software Obfuscation, Stanford University, Nov 2016.
- *Lower Bounds on VBB and Indistinguishability Obfuscations in Idealized Models.* Simons Institute for the Theory of Computing, Berkeley, August 2016.
- *Lower Bounds on Assumptions behind Indistinguishability Obfuscation.* The 3rd DC-area Crypto Day, Georgetown, May 2016.
- *Assumptions in Cryptography: How Do Cryptographers Sleep Well?* TEDx talk presented at the University of Virginia, Feb 2015.
- *On (Im)Possibility of Cryptography with Tamperable Randomness.* New York Area Crypto Day, Cornell Tech, Nov 2014.
- *Program Checkers for NP and Black-box separations (tutorial).* Summer School on Black-Box Impossibility Results, Bertinoro Italy, July 2014.
- *On (Im)Possibility of Cryptography with Tamperable Randomness.* Computer Science Department of ETH, Zurich, March 2014.

- *How to Bias Boolean Functions and Applications to Cryptographic Attacks*. Computer Science Department of Ecole Normale Supérieure (ENS) Paris, Oct 2013.
- *Time-Lock Puzzles, Proofs of Work, and Timestamping Documents*. Laboratoire d'Informatique Algorithmique (LIAFA) Paris, Oct 2013.
- *On (Im)Possibility of Tamper Resilient Cryptography*. DIMACS Workshop on Current Trends in Cryptology, New York, May 2013.
- *Time-Lock Puzzles, Proofs of Work, and Timestamping Documents*. Computer Science Colloquium, University of Montreal, April 2013.
- *On Tamper Resilient Cryptography*. Computer Science Department, University of Indiana at Bloomington, March 2013.
- *Time-Lock Puzzles, Proofs of Work, and Timestamping Documents*. ATT Research Lab, New York, January 2013.
- *On the (Im)Possibility of Tamper Resilient Cryptography*. Crypto Seminar, Computer Science Department, Boston University, Nov 2012.
- *On Efficient Zero-Knowledge PCPs*. Laboratoire d'Informatique Algorithmique (LIAFA), Paris, March 2012.
- *The Curious Case of Non-Interactive Commitments*. Computer Science Department, University of Toronto, Theory Seminar, March 2012.
- *On Efficient Zero-Knowledge PCPs*. New York's Crypto Day, Columbia University, March 2012.
- *The Curious Case of Non-Interactive Commitments*. Theory Seminar, Computer Science Department, Cornell University, Feb 2012.
- *Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography*. Computer Science Department, Columbia University, May 2010.
- *On NP-Hard Cryptography*. Computer Science Department, University of Texas at Austin, March 2010.
- *Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography*. Computer Science Department, University of Maryland, April 2010.
- *On NP-Hard Cryptography*. Computer Science Department, Cornell University, March 2010.
- *On Optimality of Merkle and Lamport Schemes*. Crypto Seminar, Computer Science Department, ETH Zurich, July 2008.
- *Merkle Puzzles are Optimal*. Institute for Advanced Study (IAS), Princeton, May 2008.
- *On Optimality of Merkle and Lamport Schemes*. Crypto Group at IBM Thomas J. Watson Research Center, March 2008.