Mohammad Mahmoody – Curriculum Vitae – April 2019

Cell number: (609) 353-6515
Email: mohammad@virginia.edu
http://www.cs.virginia.edu/~mohammad/

PO BOX 400740
85 Engineer's Way
Charlottesville, VA, USA

A Position

The University of Virginia, Charlottesville, VA, USA.
Assistant Professor in Computer Science (since August of 2013).

B Education and Training

- **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).

C Honors and Awards

- University of Virginia's SEAS Innovation Awards:
  1. *Revisiting Algorithmic Fairness and its Robustness in Adversarial Settings*, 2018.
  2. *Machine Learning in Adversarial Contexts*, 2017.
- NSF CAREER award CCF-1350939 *Separations in Cryptography*, 2014.
- Wu Prize for Excellence, Princeton University 2009.
- Ranked 1st, National Graduate Entrance Exam in Computer Science, Iran 2004.
- Gold Medal, 9th Iran National Olympiad in Informatics, Iran, 1999.

D Publication

I have listed impact factors of the journals where my work is published, but I shall add that the main venues for top work in foundations of cryptography are conferences like **Crypto, Eurocrpyt, TCC**, etc. In theoretical computer science, the custom is that the authors' names appear alphabetical order. As a result, for all publications listed below, **unless denoted by [Non-alphabetical]**, authors are in **alphabetical order**. The **underlined** authors are my students or postdocs. If the **full version** of the papers below are longer than the published version, the length of the full version and a link to the online manuscript are provided as well.

- **Journal papers**

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. (impact factor 0.735) **Full version 47 pages**, https://eprint.iacr.org/2013/194.pdf
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. (impact factor 1.021) **Full version 31 pages**, www.cs.virginia.edu/~mohammad/files/papers/MerkleFull.pdf
3. [Non-alphabetical] 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. (impact factor 1.256)
2. Saieed Akbari, Omid Etesami, Hamid Mahini, and **Mohammad Mahmoody**. *On Rainbow Cycles in Edge-Colored Complete Graphs.* Australasian Journal of Combinatorics, Vol. 37, pp. 33–42, 2007. (SJR factor 0.463)
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. (impact factor 0.557)

- **Refereed conference papers**

32. Saeed Mahloujifar, **Mohammad Mahmoody**, and Ameer Mohammed. *Universal Multi-party Poisoning Attacks.* International Conference on Machine Learning (ICML), June 2019. (acceptance rate 0.22) **Full version 22 pages**, https://arxiv.org/pdf/1809.03474.pdf
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), April 2019. (acceptance rate 0.24) **Full version 30 pages**, https://eprint.iacr.org/2018/1030.pdf
30. Saeed Mahloujifar and **Mohammad Mahmoody**. *Can Adversarially Robust Learning Leverage Computational Hardness?* Algorithmic Learning Theory (ALT), March 2019. **Full version 29 pages**, https://arxiv.org/pdf/1810.01407.pdf
29. [Non-alphabetical] 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, Jan 2019 (acceptance rate 0.16). In addition, this work was selected to be presented at NIPS 2018 Workshop on Security in Machine Learning, Dec 2018 (acceptance rate 0.27). **Full version 22 pages**, https://arxiv.org/pdf/1809.03063.pdf
28. [Non-alphabetical] 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 (NeuIPS), Dec 2018 (acceptance rate 0.20) **Full version 31 pages**, www.arxiv.org/pdf/1810.12272.pdf

27. Sanjam Garg, Mohammad Hajiabadi, **Mohammad Mahmoody**, and Ahmadreza Rahimi. *Registration-Based Encryption: Removing Private-Key Generator from IBE.* Theory of Cryptography Conference (TCC), Nov 2018. (acceptance rate 0.29) **Full version 30 pages**, https://eprint.iacr.org/2018/919.pdf

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), Springer, pp. 335–364, Aug 2018. (acceptance rate 0.22) **Full version 60 pages**, https://eprint.iacr.org/2018/555.pdf

25. Sanjam Garg, **Mohammad Mahmoody**, Daniel Masny, Izaak Meckler. *On the Round Complexity of OT Extension.* Annual International Cryptology Conference (CRYPTO), Springer, pp. 545–574, Aug 2018. (acceptance rate 0.23) **Full version 33 pages**, https://eprint.iacr.org/2017/1187.pdf

24. [Non-alphabetical] Saeed Mahloujifar, Dimitrios I. Diochnos, and **Mohammad Mahmoody**. *Learning under p-Tampering Attacks.* Algorithmic Learning Theory (ALT), pp. 572–596, April 2018. (acceptance rate 0.34) **Full version 31 pages**, https://arxiv.org/pdf/1711.03707.pdf

23. **Mohammad Mahmoody** and Saeed Mahloujifar. *Blockwise p-Tampering Attacks on Cryptographic Primitives, Extractors, and Learners.* Theory of Cryptography Conference (TCC), Springer, pp. 245–279, Nov 2017. (acceptance rate 0.34) **Full version 47 pages**, https://eprint.iacr.org/2017/950.pdf

22. Sanjam Garg and **Mohammad Mahmoody** and Ameer Mohammad. *When Does Functional Encryption Imply Obfuscation?* (acceptance rate 0.34) Theory of Cryptography Conference (TCC), Springer, pp. 82–115, Nov 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, pp. 661–695, Aug 2017 (acceptance rate 0.23) **Full version 84 pages**, https://www.cs.virginia.edu/~mohammad/files/papers/IO-all-or-nothing.pdf

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, pp. 243–272, May 2016. (acceptance rate 0.23) **Full version 33 pages**, https://eprint.iacr.org/2015/815.pdf

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, pp. 18–48, Jan 2016. (acceptance rate 0.40) **Full version 27 pages**, http://eprint.iacr.org/2015/632.pdf

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, pp. 49–66, Jan 2016. (acceptance rate 0.40)

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, pp. 462–479, Aug 2014. ***Invited to the jour-***

nal Algorithmica. (acceptance rate 0.26) **Full version 44 pages**, https://eprint.iacr.org/2013/194.pdf

16. Dana Dachman-Soled, **Mohammad Mahmoody**, Tal Malkin. *Can Optimally-Fair Coin Tossing be Based on One-Way Functions?* Theory of Cryptography Conference (TCC), Springer, pp. 217–239, Feb 2014. (acceptance rate 0.33)
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, pp. 240–264, Feb 2014. (acceptance rate 0.33) **Full version 47 pages**, https://eccc.weizmann.ac.il/report/2013/137/
14. **Mohammad Mahmoody**, Hemanta K. Maji, and Manoj Prabhakaran. *Limits of Random Oracles in Secure Computation.* Innovations in Theoretical Computer Science (ITCS), ACM, pp. 23–34, Jan 2014. (acceptance rate 0.41) **Full version 52 pages**, https://arxiv.org/pdf/1205.3554.pdf
13. **Mohammad Mahmoody** and David Xiao. *Languages with Efficient Zero Knowledge PCPs are in* SZK. Theory of Cryptography Conference (TCC), Springer, pp. 297–314, Mar 2013. (acceptance rate 0.37) ***Invited to the TCC's 10-year anniversary special issue in Computational Complexity Journal.*** **Full version 19 pages**, https://eprint.iacr.org/2012/229.pdf
12. Kai-Min Chung, Huijia Lin, **Mohammad Mahmoody**, and Rafael Pass. *On the Power of Nonuniformity in Proofs of Security.* Innovations in Theoretical Computer Science (ITCS), ACM, pp. 389–400, Jan 2013. (acceptance rate 0.39)
11. **Mohammad Mahmoody**, Tal Moran and Salil Vadhan. *Publicly Verifiable Proofs of Sequential Work.* Innovations in Theoretical Computer Science (ITCS), ACM, pp. 373–388, Jan 2013. (acceptance rate 0.39) **Full version 30 pages**, https://eprint.iacr.org/2011/553.pdf
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, pp. 701–718, Aug 2012. (acceptance 0.21) **Full version 47 pages**, www.cs.cornell.edu/~rafael/papers/NIC.pdf
9. Yuval Ishai, **Mohammad Mahmoody**, Amit Sahai. *On Efficient Zero-Knowledge PCPs.* Theory of Cryptography Conference (TCC), Springer, pp. 151–168, Mar 2012. (acceptance 0.27) ***Invited to the Journal of Cryptology***. **Full version 42 pages**, www.cs.virginia.edu/~mohammad/files/papers/ZKPCPs-Full.pdf
8. Vipul Goyal, Virendra Kumar, Satya Lokam, and **Mohammad Mahmoody**. *On Black-Box Reductions between Predicate Encryption Schemes.* Theory of Cryptography Conference (TCC), Springer, pp. 440–457, Mar 2012. (acceptance rate 0.27) **Full version 35 pages**, https://www.cs.virginia.edu/~mohammad/files/papers/12%20Predicates.pdf
7. **Mohammad Mahmoody**, Tal Moran, and Salil Vadhan. *Time-Lock Puzzles in the Random Oracle Model.* Annual Cryptology Conference (CRYPTO), Springer, pp. 39–50, Aug 2011. (acceptance rate 0.18)
6. Dana Dachman-Soled, Yehuda Lindell, **Mohammad Mahmoody**, Tal Malkin. *On the Black-Box Complexity of Optimally-Fair Coin Tossing.* Theory of Cryptography Conference (TCC), Springer, pp. 450–467, Mar 2011. (acceptance 0.32)

5. Vipul Goyal, Yuval Ishai, **Mohammad Mahmoody**, and Amit Sahai. *Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography.* Annual Cryptology Conference (CRYPTO), Springer, pp. 173–190, Aug 2010. (acceptance rate 0.19) **Full version 51 pages**, https://www.cs.virginia.edu/~mohammad/files/papers/09%20ipcp.pdf
4. **Mohammad Mahmoody** and David Xiao. *On the Power of Randomized Reductions and the Checkability of* SAT. Annual Conference on Computational Complexity (CCC), IEEE, 64–75, June 2010. (acceptance 0.32)
3. Iftach Haitner, **Mohammad Mahmoody**, and David Xiao. *A New Sampling Protocol and Applications to Basing Cryptogaphic Primitives on Hardness of* **NP**. Annual Conference on Computational Complexity (CCC), IEEE, 76–87, June 2010. (acceptance rate 0.32) **Full version 51 pages**, https://www.cs.virginia.edu/~mohammad/files/papers/07%20SamNP.pdf
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, pp. 374–390, Aug 2009. (acceptance rate 0.18) ***Invited to the Journal of Cryptology***. **Full version 31 pages**, https://www.cs.virginia.edu/~mohammad/files/papers/MerkleFull.pdf
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, Oct 2007. (acceptance 0.21) **Full version 29 pages**, https://eprint.iacr.org/2008/033.pdf

- **Manuscripts**
  - [Non-alphabetical] Mohammad Etemad, **Mohammad Mahmoody**, and David Evans. *Optimizing Trees for Static Searchable Encryption.* Cryptology ePrint 2018/052.
  - **Mohammad Mahmoody**, Ameer Mohammed, Soheil Nematihaji, Rafael Pass, and abhi shelat. *A Note on Black-Box Separations for Indistinguishability Obfuscation.* Cryptology ePrint 2016/316.
  - **Mohammad Mahmoody** and Avi Wigderson. *Black Boxes, Incorporated.*
  - **Mohammad Mahmoody**. *Studies in the Efficiency and (versus) Security of Cryptographic Tasks.* Ph.D Thesis, Princeton University, 2010.

E Citations

H-index: 14, citation count: 603, source: Google Scholar, date: March 15, 2019.

F Graduate Students

- PhD:
  1. (*Graduated*) Ameer Mohammed, 2013–2018, Assistant Professor at Kuwait University. **Supported by full scholarship from Kuwait University.**

2. Saeed Mahloujifar, 4th year, and has passed the qualifying exam.
3. Ahmadreza Rahimi, 2nd year.
4. Caleb Smith, 2nd year.

- Masters of Science:

1. (*Graduated*) Saba Eskandarian, 2015–2016, now PhD student at Stanford.
2. (*Graduated*) Soheil Nematihaji, 2014–2016, now at InMoment.

G Undergraduate Students

1. Saba Eskandarian (on depth robust graphs) 2014–2015
2. Dasith Gunawardhana (on proof of space) 2015–2016
3. Brandon Purvis (on key agreement in ROM) 2016–2017
4. Paul Sanders (on sequential functions) June 2017–2018.
5. Matthew Bielskas (on ORAM lower bounds) June 2018–now.
6. Bhuvanesh Murali (on Adversarial Machine Learning) Capstone project: Spring 2019.

H Postdocs

1. Mohammad Hajiabadi, Jan 2018 to June 2018 (still being jointly advised with Sanjam Garg).
2. Dimitris I. Diochnos, starting June 2018.

I Grants

- NSF CAREER award CCF-1350939. **$423,000** for 5 years (06/01/2014–05/31/2019).
- Making Cryptography at the Edges Made Reliable (AFORCE SUPPLEMENT). Total request $190,000 for Garg (Berkeley) and Mahmoody (UVa). UVa's share **$110,000**, awarded through a subcontract (ID 00009696) from Berkeley, (8/1/2017–7/31/2018).

J Selected Talks (Excluding Conference Presentations)

- *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 IO.* DIMACS Workshop on Complexity of Crypto 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 the (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 the (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 Superieure (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 Dept., 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 of Advanced Studies, May 2008.
- *On Optimality of Merkle and Lamport Schemes.* Crypto Group at IBM Thomas J. Watson Research Center, March 2008.

K Patents

None.

L Internal Service and Leadership

- Graduate program committee: 2018-2019.
- Chair of CS subcommittee for SEAS cybersecurity cluster search: 2017-2018.
- Committee member, SEAS cybersecurity cluster search: 2016-2017.
- Helped organize CS department's colloquium seminar series: 2016-2017.

- CS undergraduate program committee: 2014-2015, 2015-2016.
- CS outreach and diversity committees: 2014-2015, 2015-2016.
- Helped organize the SEAS open house: 2015, 2016, 2018, and 2019.
- CS graduate admissions committee: 2013-2014.
- Hosting external invited speakers to the CS department.
  - David Wu (Stanford) Spring 2018.
  - Dakshita Khurana (UCLA) Spring 2018.
  - Sampath Kannan (UPenn) Fall 2017.
  - Sanjam Garg (UC Berkeley) Fall 2017.
  - Steven Wu (Penn State) Spring 2017.
  - David Cash (Rutgers) Spring 2017.
  - John Criswell (UIUC) Spring 2014.
- PhD committees (excluding committees for the advisees):
  - Beilun Wang, PhD dissertation committee, 2017.
  - Ji Goal, PhD qualification exam committee, Spring 2018.
  - Bargav Jayaraman, PhD qualification exam committee, Spring 2018.
  - Will Hawkins, PhD qualification exam committee, Spring 2016.
  - Samee Zahur, PhD dissertation committee, March 2016.
  - Ben Terner, Master's thesis committee, Spring 2015.
  - Abbas Naderi, PhD qualification exam committee, Spring 2015.
  - Robin Künzler, ETH Zurich, external PhD committee member, 2014.
- Helped organize reading/discussion meetings on the following topics:
  - *Algorithmic Fairness*, together with CS professors Wang and Evans, SIS professor Beilin, Economics professors Nekipelov and Miller, June 2018–now.
  - *Economics and Computer Science*, together with CS professor Evans, and Economics professors Nekipelov and Miller, 2015–2016.
  - *Theoretical Topics in Computer Science*, together with CS professors Robins and Shelat, Spring 2014.
  - *Differential Privacy*, together with CS professors Evans and Gu, Spring 2017.

M Professional External Service

- **Program Committees:**
  - 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.
- **Panels:** Served in NSF Panels in 2014 and 2016.
- **Organized Workshops:**
  - Organizing (together with Iftach Haitner, Yuval Ishai, Pooya Farschim) the workshop "Lower Bounds in Cryptography", Bertinoro Italy, July 2019.
  - Helping organize Cyberwars at UVA, A GenCyber Camp, June 2018.
  - Organizing committee for DC-area crypto days:
    1. Sep 2014 at University Maryland.
    2. Oct 2015 at Johns Hopkins.
    3. May 2016 at Georgetown.
    4. May 2018 at George Mason.
- **Journal Refereeing:**
  - SIAM Journal on Computing SICOMP (2013, 2015, 2018)
  - Algorithmica (2018)
  - Quantum Information Processing (2017)
  - Journal of Information Security and Applications (2017)
  - Journal of the ACM (2017)
  - Journal of Cryptology (2013, 2015)
  - Theoretical Computer Science (2015)
  - Journal of Computing and Security (2014)
  - Before joining UVa, reviewed papers for: Theory of Computing, Transactions on Computation Theory, Random Structures and Algorithms, Cryptography and Communications, Computational Complexity Journal.