Mohammad Mahmoody

Curriculum Vitae – Jan 2016

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

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

Research Interests

Foundations of cryptography and its interplay with computational complexity.

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).

Current Position

Assistant Professor in Computer Science
The University of Virginia, Charlotesville, VA, USA (since 08/25/2013).

Honors and Awards

- NSF CAREER award CCF-1350939 *Separations in Cryptography*, 2014.
- Wu Prize for Excellence, Princeton University 2009.
- First Rank, National Graduate Entrance Examination in Computer Science, Iran 2004.
- Gold Medal, 9th Iran National Olympiad in Informatics, Iran, 1999.

Students

- Doctoral: Ameer Mohammed (done qualifying exam), Soheil Nematihaji, and Saeed Mahlouji-Far.
- Master's of Science: Saba Eskandarian
- Undergrads capstones: Saba Eskandarian (Algorithmic hardness of depth-robustness, 2014-2015) and Dasith Gunawardhana (2015-2016).

Grants

- NSF CAREER award CCF-1350939. $423,000 for 5 years (from 06/01/2014 till 05/31/2019): one month of salary each year support for one graduate student for 5 years.

Professional Service

- **Program Committees:**
  - Theory of Cryptography Conference (TCC):
    2015 Warsaw Poland. 2014 San Diego USA. 2013 Tokyo Japan. 2011 Providence USA.
  - Topics in Theoretical Computer Science (TTCS 2015).
- **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.

Publication

Conferences (accepted)

1. Mohammad Mahmoody and Ameer Mohammed *On the Power of Hierarchical Identity-Based Encryption* To appear in Eurocrypt, Vienna, Austria, May 2016. Draft available at Cryptology ePrint: http://eprint.iacr.org/2015/815.
2. Mohammad Mahmoody, Ameer Mohammed, and Soheil Nematihaji *On the Impossibility of Virtual Black-Box Obfuscation in Idealized Models* Theory of Cryptography Conference (TCC) January 2016, Tel Aviv. Draft available at Cryptology ePrint: http://eprint.iacr.org/2015/632.
3. Mohammad Mahmoody, Ameer Mohammed, Soheil Nematihaji, Rafael Pass, and abhi shelat *Lower Bounds on Assumptions behind Indistinguishability Obfuscation* Theory of Cryptography Conference (TCC) January 2016, Tel Aviv.
4. Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, Karn Seth *On the Impossibility of Cryptography with Tamperable Randomness.* CRYPTO, Lecture Notes in Computer Science, Vol. 8616, pp. 462–479, Springer, August 2014. **Invited to Algorithmica Journal**.
5. 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, February 2014.
6. 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, February 2014.
7. Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran *Limits of Random Oracles in Secure Computation.* Proc. of the 5th Conference on Innovations in Theoretical Computer Science (ITCS), pp. 23-34, January 2014.
8. Mohammad Mahmoody and David Xiao *Languages with Efficient Zero-Knowledge PCPs are in* SZK. Theory of Cryptography Conference (TCC) 2013. Springer Berlin Heidelberg, pp. 297-314, 2013.

9. Kai-Min Chung, Huijia Lin, Mohammad Mahmoody, and Rafael Pass *On the Power of Nonuniformity in Proofs of Security.* Proc. of the 4th Conference on Innovations in Theoretical Computer Science (ITCS) pp. 389-400, January 2013.

10. Mohammad Mahmoody, Tal Moran, Salil Vadhan *Publicly Verifiable Proofs of Sequential Work.* Proc. of the 4th Conference on Innovations in Theoretical Computer Science (ITCS) pp. 373-388, 2013.

11. Mohammad Mahmoody and Rafael Pass, *The Curious Case of Noninteractive Commitments, On the Power of Black-Box vs. Non-Black-Box Use of Primitives.* CRYPTO, Lecture Notes in Computer Science, Vol. 7417, pp. 701–718, Springer, 2012.)

12. Yuval Ishai, Mohammad Mahmoody, and Amit Sahai *On Efficient Zero-Knowledge PCPs.* Theory of Cryptography Conference (TCC), Lecture Notes in Computer Science, Vol. 7194, pp. 151–168, Springer, 2012. **Invited to Journal of Algorithmica**.

13. Vipul Goyal, Virendra Kumar, Satya Lokam, and Mohammad Mahmoody *On Black-Box Reductions between Predicate Encryption Schemes.* Theory of Cryptography Conference (TCC), Lecture Notes in Computer Science, Vol. 7194, pp. 440–457, Springer, 2012.

14. Mohammad Mahmoody, Tal Moran, and Salil Vadhan *Time-Lock Puzzles in the Random Oracle Model.* CRYPTO, Lecture Notes in Computer Science, Vol. 6841, pp. 39–50, Springer, 2011.

15. 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), Lecture Notes in Computer Science, Vol. 6597, pp. 450–467, Springer, 2011.

16. Vipul Goyal, Yuval Ishai, Mohammad Mahmoody, and Amit Sahai *Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography.* CRYPTO, Lecture Notes in Computer Science, Vol. 6223, pp. 173–190, Springer, 2010.

17. Mohammad Mahmoody and David Xiao *On the Power of Randomized Reductions and the Checkability of* SAT. IEEE Conference on Computational Complexity, pp. 64-75, IEEE Computer Society, 2010.

18. Iftach Haitner, Mohammad Mahmoody, and David Xiao, *A New Sampling Protocol and Applications to Basing Cryptogaphic Primitives on Hardness of* **NP**. IEEE Conference on Computational Complexity, pp. 76–87, IEEE Computer Society, 2010.

19. Boaz Barak and Mohammad Mahmoody *Merkle Puzzles are Optimal.* CRYPTO, Lecture Notes in Computer Science, Vol. 5677, pp. 374–390, Springer, 2009. **Invited to Journal of Cryptology**.

20. Boaz Barak and Mohammad Mahmoody *Lower Bounds on Signatures from Symmetric Primitives.* Proc. of IEEE Symposium on Foundations of Computer Science (FOCS), pp. 680–688, 2007.

Journals:

1. Boaz Barak and Mohammad Mahmoody *Merkles Key Agreement Protocol is Optimal.* **30 page draft.** To appear in Journal of Cryptology.

2. Amir Nayyeri, Sajjad Zarifzadeh, Nasser Yazdani, Mohammad Mahmoody, *Load sensitive topology control: Towards minimum energy consumption in dense ad hoc sensor networks.* Journal of Computer Networks, Vol. 52, pp. 493–513, 2008.

3. Saieed Akbari, Omid Etesami, Hamid Mahini, and Mohammad Mahmoody *On Rainbow Cycles in Edge-Colored Complete Graphs.* Australasian Journal of Combinatorics, Vo. 37, pp. 33–42, 2007.

4. 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:

- Mohammad Mahmoody and Avi Wigderson *Black Boxes, Incorporated.* (survey)
- Mohammad Mahmoody *Studies in the Efficiency and (versus) Security of Cryptographic Tasks* Ph.D Thesis, Princeton University, 2010.
- Kai-Min Chung, Edward Lui, Mohammad Mahmoody, and Rafael Pass *Unprovable Security of 2-Message Zero-Knowledge.*

Invited Talks

- *Assumptions in Cryptography: How Do Cryptographers Sleep Well?* ⋄ TEDx talk presented at University of Virginia, Feb 2015.
- *Tutorial Talk on Black-Box Separations.* ⋄ School on Black-Box Impossibility Results, Bertinoro Italy, July 2014.
- *On (Im)Possibility of Tamper Resilient Cryptography.* ⋄ New York Area Crypto Day, Cornell Tech, November 2014. ⋄ Computer Science Department of ETH, Zurich, March 2014. ⋄ Computer Science Department of Ecole Normale Superieure (ENS) Paris, October 2013. ⋄ DIMACS Workshop on Current Trends in Cryptology, May 2013 hold in ATT building in New York.
- *Time-Lock Puzzles, Proofs of Work, and Timestamping Documents.* ⋄ Laboratoire d'Informatique Algorithmique (LIAFA) Paris, October 2013. ⋄ ATT Research Lab, New York, January 2013. ⋄ Computer Science Department of University of Montreal, Computer Science Colloquium, April 2013.
- *On Tamper Resilient Cryptography.* University of Indiana, Computer Science Seminar, March 2013.
- *On the (Im)Possibility of Tamper Resilient Cryptography.* ⋄ Computer Science Department of Boston University, Crypto Seminar, November 2012.
- *The Curious Case of Non-Interactive Commitments.* ⋄ Computer Science Department of University of Toronto, Theory Seminar, March 2012. ⋄ Computer Science Department of Cornell University, Theory Seminar, February 2012.
- *On Efficient Zero-Knowledge PCPs.* ⋄ New York's Crypto Day at Columbia University, March 2012. ⋄ Laboratoire d'Informatique Algorithmique (LIAFA) Paris, March 2012.
- *Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography.* ⋄ Computer Science Department of Columbia University Seminar, May 2010. ⋄ Computer Science Department of University of Maryland at College Park Seminar, April 2010.
- *On NP-Hard Cryptography.* ⋄ Computer Science Department of University of Texas at Austin, Theory Seminar, March 2010. ⋄ Computer Science Department of Cornell University Theory Seminar March 2010.
- *Merkle Puzzles are Optimal.* ⋄ Institute of Advanced Studies, May 2008. ⋄ Computer Science Department of Columbia University Seminar, March 2008.
- *On Optimality of Merkle and Lamport Schemes.* ⋄ Crypto Group at IBM Thomas J. Watson Research Center, March 2008. ⋄ Crypto Group at Computer Science Department of ETH Zurich Seminar July 2008.