MAHDI CHERAGHCHI

Curriculum Vitae

Mailing address:	2260 Hayward St., Room 3603	*Phone:*	+1-734-763-9165
	Department of EECS	*Fax:*	+1-734-763-1260
	University of Michigan	*Email:*	mahdich@umich.edu
	Ann Arbor, MI 48109	*Web:*	http://mahdi.ch
	USA	*ORCID:*	0000-0001-8957-0306
		ResearcherID:	N-1367-2015

Main research Interests

- Interconnections between theoretical computer science and information and coding theory,
- Sparse recovery (e.g., compressed sensing, sparse Fourier transforms, combinatorial group testing), high dimensional geometry and their applications to algorithms for massive data,
- Information-theoretic privacy and cryptography,
- Explicit construction of combinatorial objects and derandomization theory.

Education

- **Swiss Federal Institute of Technology (EPFL)**, Lausanne, Switzerland. (November 2005 – July 2010)

  Ph.D. in Computer Science.

  Dissertation Title: *Applications of Derandomization Theory in Coding.*

  Supervisor: Amin Shokrollahi, Professor.

- **Swiss Federal Institute of Technology (EPFL)**, Lausanne, Switzerland. (October 2004 – July 2005)

  M.Sc. in Computer Science.

  Dissertation Title: *Locally Testable Codes.* (available online in ECCC thesis archive.)

  Supervisor: Amin Shokrollahi, Professor.

- **Sharif University of Technology**, Tehran, Iran. (September 2000 – July 2004)

  B.Sc. in Software Engineering and B.Sc. in Computer Hardware Engineering.

Work Experience / Affiliations

- (September 2019–*present*)
  University of Michigan, Ann Arbor: Assistant Professor of Computer Science and Engineering (CSE), Electrical Engineering and Computer Science (EECS) Department.
  - (June 2019–August 2019) Visiting Assistant Professor of CSE
  - Service assignments: Graduate Admissions Committee Member.
- (September 2019–*present*)
  Imperial College London: Honorary Senior Lecturer, Department of Computing.
- (July 2015–August 2019)
  Imperial College London: Lecturer (equivalent US term: Assistant Professor), Department of Computing.

  - Promotion to Senior Lecturer approved in 04/2019
  - (July 2017–June 2022) Member of Academic Centre of Excellence in Cyber Security Research (ACE-CSR, EPSRC grant EP/R007063/1)
  - Service assignments: Undergraduate admissions committee member, Ph.D. mentor, Ph.D. scholarships committee member, academic hiring committee member.

- (April 2015–*present*)
  Case Western Reserve University, Cleveland OH: Adjunct Assistant Professor, Department of Electrical Engineering and Computer Science.

- (January 2019–April 2019)
  Carnegie Mellon University: Visiting Faculty, Computer Science Department (hosted by Prof. Venkatesan Guruswami).

- (April 2015–June 2015)
  Qualcomm, Inc. (Qualcomm Research Berkeley): Technical consultant (Engineer II).

- (January 2015–May 2015)
  University of California, Berkeley: Visiting Assistant Project Scientist at Simons Institute for the Theory of Computing.

- (July 2013–December 2014)
  Massachusetts Institute of Technology: Post-doctoral Fellow at the Computer Science and Artificial Intelligence Lab (CSAIL) (hosted by Prof. Piotr Indyk).

- (September 2011–June 2013)
  Carnegie Mellon University: Post-doctoral Fellow at the Computer Science Department (hosted by Prof. Venkatesan Guruswami).

- (October 2010–August 2011)
  University of Texas at Austin: Post-doctoral Associate at the Department of Computer Science (hosted by Prof. David Zuckerman).

Honors, Awards and Distinctions

- (September 2016–) ACM Senior Member.
- (April 2016–) IEEE Senior Member.
- (October 2014) Qualcomm Research Fellowship.
- (June 2012) Swiss National Science Foundation Advanced Researcher Fellowship.
- (March 2011) Top 7 Doctoral Dissertations of the Year 2011 at EPFL, Switzerland (best theses are recognized annually by the EPFL Research Commission).
- (October 2010) Patrick Denantes Memorial Prize for the Best Dissertation in the School of Computer and Communication Sciences, EPFL, Switzerland.
- (May 2010) Swiss National Science Foundation Prospective Researcher Fellowship.
- (February 2005) Best B.Sc. Graduate Award in Computer Engineering, Sharif University of Technology.

Grants

- (10/2020–09/2023) National Science Foundation (NSF) CCF-2006455: "CIF: AF: Small: Data Processing Against Synchronization Errors" (sole PI, USD 489,159).
- (June 2012) Swiss National Science Foundation advanced researchers grant (No. PA00P2-141980) for the project "Coding Theory and Sparse Recovery" (USD 76,700).
- (May 2010) Swiss National Science Foundation prospective researchers grant (No. PBELP2-133367) for the project "Pseudorandomness, Extractor Theory, and Coding" (USD 66,500).

Granted Patents

1. Thomas Richardson, Michael Luby, Mahdi Cheraghchi, Lorenz Minder. (Qualcomm, Inc.) *Systems and methods for verification of code resiliency for data storage.* United States Patent 10,003,357, June 19, 2018.

Outreach

1. (October 2018) Interview with Faculti website on information theory research (available at `https://faculti.net/capacity-upper-bounds-deletion-type-channels`).

PhD Student Supervision

1. Alexandra Veliche (September 2020–)
2. Joseph Downs (September 2020–)
3. João Ribeiro (October 2017–)
4. Dimitrios Myrisiotis (October 2017–)

Visiting PhD Students

1. Thach Van Bui from SOKENDAI (The Graduate University for Advanced Studies), Japan (October 2017).

Research Publications

All publications are available online at `http://mahdi.cheraghchi.info/writings/`.
*Five selected publications are marked with asterisks.

Journal Papers

[1] M. Cheraghchi, V. Kabanets, Z. Lu, D. Myrisiotis. *Circuit Lower Bounds for MCSP from Local Pseudorandom Generators.* ACM Transactions on Computation Theory **(ToCT)** 12(3), DOI: 10.1145/3404860, (extended version of [26]), 2020.

[2] M. Cheraghchi. J. Ribeiro. *An Overview of Capacity Results for Synchronization Channels.* **IEEE Transactions** on Information Theory, DOI:10.1109/TIT.2020.2997329, 2020.

[3] M. Cheraghchi, R. Gabrys, O. Milenkovic, J. Ribeiro. *Coded Trace Reconstruction.* **IEEE Transactions** on Information Theory (extended version of [25]), DOI:10.1109/TIT.2020.2996377, 2020.

[4] M. Cheraghchi. J. Ribeiro. *Sharp Analytical Capacity Upper Bounds for Sticky and Related Channels.* **IEEE Transactions** on Information Theory 65(11), pp. 6950–6974, DOI:10.1109/TIT.2019.2920375 (extended version of [30]), 2019.

[5] T. V. Bui, M. Kuribayashi, M. Cheraghchi, I. Echizen. *Efficiently Decodable Non-Adaptive Threshold Group Testing.* **IEEE Transactions** on Information Theory 65(9), pp. 5519–5528, DOI:10.1109/TIT.2019.2907990 (extended version of [33]), 2019.

*[6] M. Cheraghchi. *Capacity Upper Bounds for Deletion-Type Channels.* Journal of the ACM **(JACM)** 6(2):9, DOI: 10.1145/3281275 (extended version of [34]), 2019.

[7] M. Cheraghchi. *Expressions for the Entropy of Basic Discrete Distributions.* **IEEE Transactions** on Information Theory 65(7), pp. 3999–4009, DOI:10.1109/TIT.2019.2900716 (extended version of [32]), 2019.

[8] M. Cheraghchi, J. Ribeiro. *Improved Upper Bounds and Structural Results on the Capacity of the Discrete-Time Poisson Channel.* **IEEE Transactions** on Information Theory 65(7), pp. 4052–4068, DOI:10.1109/TIT.2019.2896931 (extended version of [31]), 2019.

[9] M. Cheraghchi. *Nearly Optimal Robust Secret Sharing.* **Designs, Codes and Cryptography** 87(8), pp. 1777–1796, DOI:10.1007/s10623-018-0578-y (extended version of [37]), 2019.

[10] M. Cheraghchi, E. Grigorescu, B. Juba, K. Wimmer, N. Xie. $\mathrm{AC}^0 \circ \mathrm{MOD}_2$ *lower bounds for the Boolean Inner Product,* Journal of Computer and System Sciences **(JCSS)** vol. 97, pp. 45–59, 2018 (extended version of [36]).

[11] K. Chandrasekaran, M. Cheraghchi, V. Gandikota, E. Grigorescu. *Local Testing of Lattices.* SIAM Journal on Discrete Mathematics **(SIDMA)** 32(2), pp. 1265-1295, 2018 (extended version of [35]).

*[12] M. Cheraghchi, P. Indyk. *Nearly Optimal Deterministic Algorithm for Sparse Walsh-Hadamard Transform.* ACM Transactions on Algorithms **(TALG)** 13(3):34, 2017 (extended version of [38]).

*[13] M. Cheraghchi, V. Guruswami. *Non-Malleable Coding Against Bit-wise and Split-State Tampering.* **Journal of Cryptology** 30(1), pp. 191–241, 2017 (extended version of [39]).

*[14] M. Cheraghchi, V. Guruswami. *Capacity of Non-Malleable Codes.* **IEEE Transactions** on Information Theory 62(3), pp. 1097–1118, 2016 (extended version of [40]).

*[15] M. Cheraghchi, V. Guruswami, A. Velingker. *Restricted Isometry of Fourier Matrices and List Decodability of Random Linear Codes.* SIAM Journal on Computing **(SICOMP)** 42(5), pp. 1888–1914, 2013. arXiv:1207.1140 (extended version of [41]).

[16] M. Cheraghchi. *Improved Constructions for Non-adaptive Threshold Group Testing.* **Algorithmica** 67(3), pp. 384–417, 2013. arXiv:1002.2244, DOI: 10.1007/s00453-013-9754-7. (extended version of [46]).

[17] M. Cheraghchi. *Noise-Resilient Group Testing: Limitations and Constructions.* **Discrete Applied Mathematics** 161(1–2), pp. 81–95, 2013. DOI: 10.1016/j.dam.2012.07.022, arXiv:0811.2609 (extended version of [49]).

[18] M. Cheraghchi, J. Håstad, M. Isaksson, O. Svensson. *Approximating Linear Threshold Predicates.* ACM Transactions on Computation Theory **(ToCT)** 4(1), Article 2, March 2012. ECCC TR10-132 (extended version of [45]).

[19] M. Cheraghchi, F. Didier, A. Shokrollahi. *Invertible Extractors and Wiretap Protocols.* **IEEE Transactions** on Information Theory 58(2), pp. 1254–1274, 2012. arXiv:0901.2120 (extended version of [51]).

[20] M. Cheraghchi, A. Karbasi, S. Mohajer, V. Saligrama. *Graph-Constrained Group Testing.* **IEEE Transactions** on Information Theory 58(1), pp. 248–262, 2012. arXiv:1001.1445 (extended version of [47]).

[21] M. Cheraghchi, A. Hormati, A. Karbasi, M. Vetterli. *Compressed Sensing with Probabilistic Tests: Theory, Design and Application.* **IEEE Transactions** on Information Theory 57(10), pp. 7057–7067, 2011. (arXiv:1009.3186, extended version of [48]).

Conference Papers

[22] M. Cheraghchi and V. Nakos. *Combinatorial Group Testing Schemes with Near-Optimal Decoding Time.* In Proceedings of the 61st Annual IEEE Symposium on Foundations of Computer Science **(FOCS)**, 2020.

[23] T. V. Bui, M. Cheraghchi, I. Echizen. *Improved Non-adaptive algorithms for Threshold Group Testing with a Gap.* In Proceedings of the IEEE International Symposium on Information Theory **(ISIT)**, 2020.

[24] F. Lin, M. Cheraghchi, V. Guruswami, R. Safavi-Naini, H. Wang. *Leakage-Resilient Secret Sharing in Non-compartmentalized Models*. In Proceedings of the Conference on Information-Theoretic Cryptography **(ITC)**, 2020.

[25] M. Cheraghchi, R. Gabrys, O. Milenkovic, J. Ribeiro. *Coded Trace Reconstruction*. In Proceedings of the IEEE Information Theory Workshop **(ITW)**, arXiv:1903.09992, 2019.

[26] M. Cheraghchi, V. Kabanets, Z. Lu, D. Myrisiotis. *Circuit Lower Bounds for MCSP from Local Pseudorandom Generators.* In Proceedings of the 46th International Colloquium on Automata, Languages and Programming **(ICALP)**, 2019.

[27] M. Cheraghchi. J. Ribeiro. *Simple Codes and Sparse Recovery with Fast Decoding*. In Proceedings of the IEEE International Symposium on Information Theory **(ISIT)**, 2019.

[28] F. Lin, R. Safavi-Naini, M. Cheraghchi, H. Wang. *Non-Malleable Codes against Active Physical Layer Adversary.* In Proceedings of the IEEE International Symposium on Information Theory **(ISIT)**, 2019.

[29] F. Lin and M. Cheraghchi and V. Guruswami and R. Safavi-Naini and H. Wang. *Secret Sharing with Binary Shares.* In Proceedings of the 10th Innovations in Theoretical Computer Science Conference **(ITCS)**, arXiv:1808.02974, 2019.

[30] M. Cheraghchi. J. Ribeiro. *Sharp Analytical Capacity Upper Bounds for Sticky and Related Channels.* In Proceedings of the 56th Annual **Allerton** Conference on Communication, Control, and Computing, 2018.

[31] M. Cheraghchi. J. Ribeiro. *Improved Capacity Upper Bounds for the Discrete-Time Poisson Channel.* In Proceedings of the IEEE International Symposium on Information Theory **(ISIT)**, 2018.

[32] M. Cheraghchi. *Expressions for the entropy of binomial-type distributions.* In Proceedings of the IEEE International Symposium on Information Theory **(ISIT)**, 2018.

[33] T. V. Bui, M. Kuribayashi, M. Cheraghchi, I. Echizen. *Efficiently Decodable Non-Adaptive Threshold Group Testing.* In Proceedings of the IEEE International Symposium on Information Theory **(ISIT)**, 2018.

[34] M. Cheraghchi. *Capacity Upper Bounds for Deletion-Type Channels.* In Proceedings of the 50th ACM Symposium on Theory of Computing **(STOC)**. arXiv:1711.01630, 2018.

[35] K. Chandrasekaran, M. Cheraghchi, V. Gandikota, E. Grigorescu. *Local Testing for Membership in Lattices.* In Proceedings of the 36th Foundations of Software Technology and Theoretical Computer Science conference **(FSTTCS)**, 2016.

[36] M. Cheraghchi, E. Grigorescu, B. Juba, K. Wimmer, N. Xie. $\mathrm{AC}^0 \circ \mathrm{MOD}_2$ *lower bounds for the Boolean Inner Product,* In Proceedings of the 43rd International Colloquium on Automata, Languages and Programming **(ICALP)**, 2016.

[37] M. Cheraghchi. *Nearly Optimal Robust Secret Sharing.* In Proceedings of the IEEE International Symposium on Information Theory **(ISIT)**, 2016.

[38] M. Cheraghchi, P. Indyk. *Nearly Optimal Deterministic Algorithm for Sparse Walsh-Hadamard Transform.* In Proceedings of the ACM-SIAM Symposium on Discrete Algorithms **(SODA)**. ECCC TR15-076, 2016.

[39] M. Cheraghchi, V. Guruswami. *Non-Malleable Coding Against Bit-wise and Split-State Tampering.* In Proceedings of Theory of Cryptography Conference **(TCC)**. ECCC TR13-121, 2014.

[40] M. Cheraghchi, V. Guruswami. *Capacity of Non-Malleable Codes.* In Proceedings of Innovations in Theoretical Computer Science **(ITCS)**. ECCC TR13-118, 2014.

[41] M. Cheraghchi, V. Guruswami, A. Velingker. *Restricted Isometry of Fourier Matrices and List Decodability of Random Linear Codes.* In Proceedings of the ACM-SIAM Symposium on Discrete Algorithms **(SODA)**. arXiv:1207.1140, 2013.

[42] M. Cheraghchi, A. Klivans, P. Kothari, H.K. Lee. *Submodular Functions Are Noise Stable.* In Proceedings of the ACM-SIAM Symposium on Discrete Algorithms **(SODA)**, 2012. arXiv:1106.0518.

[43] M. Cheraghchi. *Coding-Theoretic Methods for Sparse Recovery.* In Proceedings of 49th **Allerton** Conference on Communication, Control and Computing, 2011 (invited paper).

[44] M. Cheraghchi. *Derandomization and Group Testing.* In Proceedings of 48th **Allerton** Conference on Communication, Control and Computing, 2010 (invited paper).

[45] M. Cheraghchi, J. Håstad, M. Isaksson, O. Svensson. *Approximating Linear Threshold Predicates.* In Proceedings of the 13th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems **(APPROX)**, 2010.

[46] M. Cheraghchi. *Improved Constructions for Non-adaptive Threshold Group Testing.* In Proceedings of the 37th International Colloquium on Automata, Languages and Programming **(ICALP)**, 2010.

[47] M. Cheraghchi, A. Karbasi, S. Mohajer, V. Saligrama. *Graph-Constrained Group Testing.* In Proceedings of IEEE International Symposium on Information Theory **(ISIT)**, 2010 (*nominated for the best student paper award.*

[48] M. Cheraghchi, A. Hormati, A. Karbasi, M. Vetterli. *Compressed Sensing with Probabilistic Measurements: A Group Testing Solution.* In Proceedings of 47th **Allerton** Conference on Communication, Control and Computing, 2009.

[49] M. Cheraghchi. *Noise-Resilient Group Testing: Limitations and Constructions.* In Proceedings of 17th International Symposium on Fundamentals of Computation Theory **(FCT)**, 2009.

[50] M. Cheraghchi. *Capacity Achieving Codes from Randomness Conductors.* In Proceedings of IEEE International Symposium on Information Theory **(ISIT)**, 2009.

[51] M. Cheraghchi, F. Didier, A. Shokrollahi. *Invertible Extractors and Wiretap Protocols.* In Proceedings of IEEE International Symposium on Information Theory **(ISIT)**, 2009.

[52] E. Ardestanizadeh, M. Cheraghchi, A. Shokrollahi. *Bit Precision Analysis for Compressed Sensing.* In Proceedings of IEEE International Symposium on Information Theory **(ISIT)**, 2009.

[53] M. Cheraghchi, A. Shokrollahi. *Almost-Uniform Sampling of Points on High-Dimensional Algebraic Varieties.* In Proceedings of 26th International Symposium on Theoretical Aspects of Computer Science **(STACS)**, 2009.

[54] M. Cheraghchi, A. Shokrollahi, A. Wigderson. *Computational Hardness and Explicit Constructions of Error Correcting Codes.* In Proceedings of 44th **Allerton** Conference on Communication, Control and Computing, 2006 (invited paper).

Technical Reports and Preprints in Submission

[55] M. Cheraghchi, S. Hirahara, D. Myrisiotis, and Y. Yoshida. *One-Tape Turing Machine and Read-Once Branching Program Lower Bounds for MCSP.* Submitted, 2020.

[56] M. Cheraghchi, E. Grigorescu, B. Juba, K. Wimmer, and N. Xie. *List Learning with Attribute Noise.* Submitted, 2020.

[57] T. V. Bui, M. Kuribayashi, M. Cheraghchi and I. Echizen. *Efficient and error-tolerant schemes for non-adaptive complex group testing and its application in complex disease genetics*. arXiv:1904.00349, 2019.

[58] T. V. Bui, M. Kuribayashi, M. Cheraghchi, I. Echizen. *Improved Encoding and Decoding for Non-Adaptive Threshold Group Testing.* arXiv:1901.02283, 2019.

[59] T. V. Bui, M. Kuribayashi, M. Cheraghchi and I. Echizen. *A framework for generalized group testing with inhibitors and its potential application in neuroscience*. arXiv:1810.01086, 2018.

[60] M. Cheraghchi, A. Gál, A. Mills. *Bounds on Correctness and Corruption for Locally Decodable Codes.* ECCC TR12-172, 2012.

[61] M. Cheraghchi. *On Matrix Rigidity and the Complexity of Linear Forms.* ECCC TR05-070, 2005.

Teaching (as an instructor)

- At the University of Michigan–Ann Arbor:
  - (Fall 2020) EECS 598: Randomness and Computation.
  - (Winter 2020, Winter 2021) EECS 475: Introduction to Cryptography.
  - (Fall 2019) EECS 498/598: Coding Theory for Theoretical Computer Science.
- At Imperial College London, Department of Computing:
  - (Autumn 2018) CO-202: Algorithms II.
  - (Autumn 2016, Autumn 2017) CO-484: Quantum Computing. Joint with Dr. Herbert Wiklicky.
  - (Autumn 2015, Autumn 2016, Autumn 2017, Autumn 2018) CO-349: Information and Coding Theory. Joint with Dr. Herbert Wiklicky.
  - (Autumn 2015, Autumn 2016, Autumn 2017) CO-145: Mathematical Methods. Joint with Dr. Marc Deisenroth.
- At MIT EECS:
  - (Fall 2014) 6.006: Introduction to Algorithms. Joint with Profs. Silvio Micali and Vinod Vaikuntanathan.
  - (Spring 2014) 6.045: Automata, Computability, and Complexity. Joint with Prof. Madhu Sudan.
- At CMU Computer Science Department:
  - (Spring 2013) 15-859: Introduction to Information Theory and its Applications in Theory of Computation. Joint with Prof. Venkatesan Guruswami.

Academic Service

- Technical program committee member:
  1. The 2021 IMA International Conference on Cryptography and Coding.
  2. The 2020 IEEE Information Theory Workshop (ITW 2020).
  3. The 2020 IEEE International Symposium on Information Theory (ISIT 2020).
  4. The 45th Mathematical Foundations of Computer Science (MFCS 2020).
  5. The First Conference on Information Theoretic Cryptography (ITC 2020).
  6. The 2019 IEEE International Symposium on Information Theory (ISIT 2019).
  7. The 2018 IEEE International Symposium on Information Theory (ISIT 2018).
  8. The 20th International Workshop on Randomization and Computation (RANDOM 2016).
- USA National Science Foundation (NSF) panelist, 2019.
- (06/2017–*present*) Reviewer for American Mathematical Society (AMS) Mathematical Reviews.
- (10/2016–*present*) EPSRC (Engineering and Physical Sciences Research Council) College Member, UK (10/2016–02/2018 Associate College Member). Responsibilities include peer-review of proposals for research funding and serving on prioritization panels.
- (03/2015) Co-organizer of the DIMACS Workshop on "Coding Theoretic Methods for Network Security" (a part of the DIMACS Special Focus on Cybersecurity), March 25–27, 2015.
- (11/2011–03/2016) Editorial board member, International Journal of Information and Coding Theory, ISSN 1753-7703 / 1753-7711.
- Served as reviewer for
  - Journals: Journal of the ACM (JACM), SIAM Journal on Computing (SICOMP), IEEE Transactions on Information Theory (IEEE IT), ACM Transactions on Algorithms, Computational Complexity, Journal of Fourier Analysis and Applications (JFAA), Communications on Pure and Applied Mathematics, IEEE Transactions on Signal Processing, Theoretical Computer Science, Discrete Applied Mathematics (DAM), IEEE Journal on Selected Areas in Communications (JSAC), ACM Transactions on Sensor Networks, Optimization Letters (Springer), Signal Processing, Information Processing Letters (IPL), Information Sciences, Scientia Iranica.
  - Conferences: IEEE Symposium on Foundations of Computer Science (FOCS 2012, 2015, 2016, 2017, 2019), ACM Symposium on the Theory of Computing (STOC 2014, 2017, 2020), ACM-SIAM Symposium on Discrete Algorithms (SODA 2013, 2018, 2019, 2020, 2021), International Cryptology Conference (CRYPTO 2015, 2020), IEEE Conference on Computational Complexity (CCC 2012), Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2017, 2019), Theory of Cryptography Conference (TCC 2012, 2016), International Colloquium on Automata, Languages and Programming (ICALP 2016), Symposium on Theoretical Aspects of Computer Science (STACS 2012, 2015), Innovations in Theoretical Computer Science (ITCS 2019), International Workshop on Randomization and Computation (RANDOM 2011, 2016, 2018), International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX 2015), IEEE International Symposium on Information Theory (ISIT 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2015, 2017, 2018, 2020), IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2017), International Conference on Cryptology and Information Security in Latin America (Latincrypt 2015), International Symposium on Algorithms and Computation (ISAAC 2012), IEEE Information Theory Workshop (ITW 2016, 2018), International Symposium on Turbo Codes and Related Topics (Turbo 2008), IMA Conference on Cryptography and Coding (2007).
  - Funding schemes: Swiss National Science Foundation (2016), BSF (2019), ISF (2020), Engineering and Physical Sciences Research Council (EPSRC UK, 2016, 2017).

- Session chair: ITA (Information Theory and Applications Workshop) 2012, 2013, and 2018, International Conference on Topics in Theoretical Computer Science (TTCS 2017), IEEE International Symposium on Information Theory (ISIT 2018), Conference on Information Theoretic Cryptography (ITC 2020).
- Invited participant in the "TCS Visioning Workshop" of the Committee for the Advancement of Theoretical Computer Science (CATCS), 2020.
- PhD defense committee: Dawei Huang (03/2020, U. of Michigan CSE).

Invited Research Talks

- Invited talks at the 2020, 2019, 2018, 2016, 2015, 2014, 2013, 2012, 2011 Information Theory and Applications (ITA) Workshop, University of California, San Diego, CA (February each year).
- Invited speaker at *Workshop on Coding and Information Theory*, Center of Mathematical Sciences and Application, Harvard University (04/2018).
- "Capacity Upper Bounds for Deletion-Type Channels". Invited talk at Case Western Reserve University (04/2018, hosted by Prof. Harold Connamacher) and Centre for Discrete Mathematics and its Applications at the University of Warwick (10/2018).
- Colloquium speaker at School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran (09/2017).
- Keynote speaker at the second International Conference on Topics in Theoretical Computer Science (TTCS 2017), Tehran, Iran (09/2017).
- Invited talk at Workshop on Mathematics of Information-Theoretic Cryptography, Institute for Mathematical Sciences, National University of Singapore (09/2016).
- "Nearly Optimal Robust Secret Sharing". At Simons Institute for the Theory of Computing, University of California, Berkeley (06/2016).
- "Nearly Optimal Deterministic Algorithm for Sparse Walsh-Hadamard Transform". Invited talks at IBM T.J. Watson Research Center (09/2018, hosted by Dr. Krzysztof Onak), University of Oxford (05/2017, hosted by Dr. Standa Živný), University of Toronto (02/2017), Case Western Reserve University (05/2015, hosted by Prof. Harold Connamacher), and the iCORE Information Security Laboratory, University of Calgary (08/2015, hosted by Prof. Rei Safavi-Naini).
- "Non-Malleable Codes: Applications and Constructions." Invited talks at Case Western Reserve University (11/2014, hosted by Prof. Harold Connamacher), and the iCORE Information Security Laboratory, University of Calgary (08/2015, hosted by Prof. Rei Safavi-Naini).
- Invited talk at the 2015 AMS/MAA Joint Mathematics Meetings (JMM), San Antonio, TX (01/2015).
- Invited speaker at the 52nd Allerton Conference on Communication, Control and Computing, Allerton Retreat Center, Monticello, Illinois (09/2014).
- "New Faces of Error-Correcting Codes". Invited talks at University of Central Florida (02/2014), ETHZ (02/2014), Imperial College London (03/2014) and University of California, Davis (04/2014).
- "Non-Malleable Coding Against Bit-wise and Split-State Tampering". Invited talks at New York University (11/2013, hosted by Prof. Yevgeniy Dodis), Northeastern University (11/2013, hosted by Prof. Daniel Wichs), and ETHZ (02/2014, hosted by Prof. Ueli Maurer).
- "Capacity and Constructions of Non-Malleable Codes". Invited talks at the MIT Theory of Computation (TOC) Seminar (12/2013), Carnegie Mellon University (11/2013, hosted by Prof. Venkatesan Guruswami), New York City Crypto Day (11/2013, held in New York University and hosted by Dr. Tal Rabin and Dr. Sanjam Garg), IBM T.J. Watson Research Center (11/2013, hosted by Dr. Krzysztof Onak), and Bell Laboratories (11/2013, hosted by Dr. Emina Soljanin), McGill University (01/2014, hosted by Prof. Hamed Hatami), Purdue University (10/2014, hosted by Prof. Elena Grigorescu).

- "Restricted Isometry of Fourier Matrices and List Decodability of Random Linear Codes". Invited talk at Coordinated Science Laboratory, University of Illinois at Urbana-Champaign (02/2013, hosted by Prof. Olgica Milenkovic).
- "Restricted Isometry of Fourier Matrices and List Decodability of Random Linear Codes". Invited talk at Bell Laboratories, Murray Hill, NJ (10/2012, hosted by Dr. Emina Soljanin).
- Invited lecture at the University of Michigan, Ann Arbor for "Coding, Complexity, and Sparsity Workshop" (07/2012).
- Invited lecture at the Institute for Mathematics and Its Applications (IMA) at the University of Minnesota for workshop "Group Testing Designs, Algorithms, and Applications to Biology" (02/2012).
- Invited talk at the Department of Computer Science and Engineering, Pennsylvania State University (11/2011, hosted by Prof. Martin Fürer).
- Invited speaker at the 49th Allerton Conference on Communication, Control and Computing, Allerton Retreat Center, Monticello, Illinois (09/2011).
- "Derandomization and Group Testing". Invited talk at the 48th Allerton Conference on Communication, Control and Computing, Allerton Retreat Center, Monticello, Illinois (09/2010).
- "Noise-Resilient Group Testing: Limitations and Constructions" at Institute for Advanced Study, Princeton (01/2009); MIT CSAIL (01/2009); UC Berkeley (01/2009).
- "Invertible Extractors and Wiretap Protocols" at Princeton University (01/2009); UC San Diego (01/2009).

Student Project Supervision

Undergraduate student projects supervised at the University of Michigan (2019–):

1. "A structural study of good error-correcting codes": UROP project by Yuxuan Chen, Yiwen Ding, Jonah Nan (2019–2020).
2. "Haskell Implementation of Lattice-Cryptographic Key-Homomorphic Pseudorandom Function" Honors Capstone project by Bogdan Manga (2019–2020).
3. Vinod Raman and Sanjana Kolisetty (Summer 2020).

Masters theses supervised at Imperial College London (2015-2019):

1. "Algorithms for Graph Partitioning" by Shahrokh Shahi, 2016.
2. "Problems and reductions in lattice-based cryptography" by Liu Wing Sang Vincent, 2016.

Student individual and group projects supervised at Imperial College London (2015-2019):

1. "Secure two-party computation using garbled circuits" by Ignacio Navarro. MEng individual project, Spring 2018.
2. "ShareRoom" by Oana Ciocioman, Cristian Matache, Silvia Sapora, Alexandru Toma, Andrei Puiu, Vlad Hadarean. Software Engineering group project, Autumn 2017.
3. "MapNotes" by Dennis Tsiang, Harry Moore, Thomas Allerton, Tanmay Khanna, Adanna Akwataghibe, Shiraz Butt. Software Engineering group project, Autumn 2017.
4. "Cross-platform mobile application: Platform for borrowing and lending items" by Ashwitha Bingumalla, Timan Noel, Krishi Shah, Nikhita Vasani, Masturah Wan Mohd Azmi. BEng group project, Autumn 2016.

5. "Dether: A platform for incentive-driven sharing of smart contracts on the Ethereum blockchain" by Mateusz Dyda (MEng), Spring 2016.
6. "How to flip coins" by Jason Yu (BEng, Spring 2017), Adam Hosier (BEng, Spring 2017).
7. "Extracting Randomness From Independent Sources" by Xin Chen (MEng), Spring 2016.
8. "Cellular Automata" by Miguel Marques (BEng), Spring 2016.
9. "Data Structure Visualizations" by Yuliya Gitlina (BEng, Spring 2016), Andrea Janoscikova (BEng, Spring 2017), Rosita Rodrigues (BEng, Spring 2017).
10. "Extracting Information from Cryptocurrency" by Lim Zun Yuan (BEng), Spring 2016.
11. "Sharify: an online sharing platform" by Georg Grob, Kunal Wagle, Andrew Poor, Krish De Souza, Mazen El-Turk. 3rd year group project, Autumn 2015.

References (in alphabetical order)

1. Venkatesan Guruswami, Professor, Computer Science Department, Carnegie Mellon University, Pittsburgh PA 15213, USA.
email: venkatg@cs.cmu.edu, *phone:* +1(412)268-4899.
2. Piotr Indyk, Professor, MIT Computer Science and Artificial Intelligence Lab, Cambridge MA 02139, USA.
email: indyk@mit.edu, *phone:* +1(617)452-3402.
3. Michael Mitzenmacher, Professor, School of Engineering and Applied Sciences Harvard University, Cambridge, MA 02138, USA.
email: michaelm@eecs.harvard.edu, *phone:* +1(617)496-7172.
4. Amin Shokrollahi, Professor, School of Computer and Communication Sciences (IC) and Faculty of Basic Sciences (FSB), Swiss Federal Institute of Technology, Lausanne, Switzerland.
email: amin.shokrollahi@epfl.ch, *phone:* +41(21)693-7512.