MAHDI CHERAGHCHI

Curriculum Vitae

Mailing address: Department of Computing
Imperial College London
Huxley Building, Room 450
180 Queen's Gate
London SW7 2RH, UK
Phone: +44(0)20 7594 8216
Fax: +44(0)20 7594 8282

Email: m.cheraghchi@imperial.ac.uk
Web: http://cheraghchi.info

Citizenship: Iran
USA Permanent Resident

Research Interests

In a broad sense: Theoretical Computer Science, Coding and Information Theory, Signal Processing. In particular:

- Interconnections between electrical engineering and theoretical computer science,
- Sparse recovery (e.g., compressive sensing and combinatorial group testing) and high-dimensional geometry,
- Information-theoretic privacy and security,
- Derandomization, pseudorandomness and explicit construction of combinatorial objects,
- Probabilistically Checkable Proofs, hardness of approximation and their connections with Boolean analysis.

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.

  GPA: 5.94 / 6.00 .

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

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

  B.Sc. Dissertation: *Human Face Localization in Still Color Images.*

  Dissertation Advisor: Mansour Jamzad, Associate Professor.

  GPA: 19.06 / 20.00 — Ranked First by the Education Bureau.

Work Experience / Affiliations

- (July 2015–*present*)
  Imperial College London: Lecturer (equivalent US term: Assistant Professor), Department of Computing.
- (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).
- (August 2009–October 2009)
  Royal Institute of Technology (KTH), Sweden: Visiting Student Researcher at the Computer Science Department (Research on Hardness of Approximation under supervision of Prof. Johan Håstad).

Honors, Awards and Distinctions

- (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.
- (May 2004, May 2003) Second (resp. Third) Place, Nationwide Examination for Graduate Admissions in Computer Science, Iran.
- (August 2000) Ranked 115 Among Over 350'000 in the Nationwide Examination for Undergraduate Admissions in the Public Universities, Iran.

Grants

- (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).

Research Publications

(all publications are available online at `http://mahdi.ch/writings`)

Journal Papers

[1] M. Cheraghchi, V. Guruswami. *Capacity of Non-Malleable Codes.* Accepted for publication in IEEE Transactions on Information Theory (extended version of [10]), 2015.

[2] M. Cheraghchi, V. Guruswami, A. Velingker. *Restricted Isometry of Fourier Matrices and List Decodability of Random Linear Codes.* SIAM Journal on Computing 42(5), pp 1888–1914, 2013. arXiv:1207.1140 (extended version of [11]).

[3] 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 [16]).

[4] 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 [19]).

[5] M. Cheraghchi, J. Håstad, M. Isaksson, O. Svensson. *Approximating Linear Threshold Predicates.* ACM Transactions on Computation Theory 4(1), Article 2, March 2012. ECCC TR10-132 (extended version of [15]).

[6] 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 [21]).

[7] 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 [17]).

[8] 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 [18]).

Conference Papers

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

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

[11] 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 2013). arXiv:1207.1140, 2013.

[12] 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), 2012. arXiv:1106.0518.

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

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

[15] 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.

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

[17] 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.*

[18] 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.

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

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

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

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

[23] 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.

[24] 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 / Preprints

[25] K. Chandrasekaran, M. Cheraghchi, V. Gandikota, E. Grigorescu. *Local Testing of Lattices.* 2015.

[26] M. Cheraghchi, P. Indyk. *Nearly Optimal Deterministic Algorithm for Sparse Walsh-Hadamard Transform.* ECCC TR15-076, 2015.

[27] M. Cheraghchi, E. Grigorescu, B. Juba, K. Wimmer, N. Xie. $\mathrm{AC}^0 \circ \mathrm{MOD}_2$ *lower bounds for the Boolean Inner Product,* ECCC TR15-030, 2015.

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

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

Theses

[30] M. Cheraghchi. *Applications of Derandomization Theory in Coding.* Ph.D. Thesis No. 4767, EPFL, Switzerland. arXiv:1107.4709. 2010.

[31] M. Cheraghchi. *Locally Testable Codes.* M.Sc. Thesis, EPFL, Switzerland. 2005.

[32] M. Cheraghchi. *Human Face Localization in Still Color Images.* B.Sc. Dissertation (in Persian), Sharif University of Technology, Tehran, Iran. 2004.

Teaching

- (Fall 2014) Instructor for "6.006: Introduction to Algorithms". Department of Electrical Engineering and Computer Science, MIT. An undergraduate course jointly taught with Profs. Silvio Micali and Vinod Vaikuntanathan.
- (Spring 2014) Instructor for "6.045: Automata, Computability, and Complexity". Department of Electrical Engineering and Computer Science, MIT. An undergraduate course jointly taught with Prof. Madhu Sudan.
- (Spring 2013) Instructor for "15-859: Introduction to information theory and its applications in theory of computation". Computer Science Department, Carnegie Mellon University. A graduate-level course jointly designed with Prof. Venkatesan Guruswami.
- (2005 – 2009) Teaching Assistant, Swiss Federal Institute of Technology, Lausanne. Courses: Linear Algebra (Winter 2005), Undergraduate algorithms (Summer 2006, Winter 2007, Fall 2009), Graduate algorithms (Winter 2006, Summer 2007), Coding theory (Summer 2009).
- (2001 – 2003) Teaching Assistant, Department of Computer Engineering, Sharif University of Technology. Courses: Design and Implementation of the Programming Languages (Fall 2003), Microprocessors (Spring 2003), Data Structures and Algorithms (Spring 2003), Structured C Programming (Fall 2002), Computer Programming in Pascal (Fall 2001, Spring 2002).

Academic Service

- (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.
- Editorial board member, International Journal of Information and Coding Theory, ISSN 1753-7703 / 1753-7711 (11/2011–*present*).
- Served as reviewer for
  - Journals: Information Processing Letters (IPL), IEEE Journal on Selected Areas in Communications (JSAC), SIAM Journal on Computing (SICOMP), Discrete Applied Mathematics (DAM), IEEE Transactions on Information Theory (IEEE IT), ACM Transactions on Sensor Networks, IEEE Transactions on Signal Processing, Optimization Letters (Springer), Journal of the ACM (JACM), ACM Transactions on Algorithms.
  - Conferences: IMA Conference on Cryptography and Coding (2007), International Symposium on Turbo Codes and Related Topics (Turbo 2008), IEEE International Symposium on Information Theory (ISIT 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2015), International Workshop on Randomization and Computation (RANDOM 2011), Symposium on Theoretical Aspects of Computer Science (STACS 2012, 2015), Theory of Cryptography Conference (TCC 2012), IEEE Conference on Computational Complexity (CCC 2012), IEEE Symposium on Foundations of Computer Science (FOCS 2012, 2015), ACM-SIAM Symposium on Discrete Algorithms (SODA 2013), International Symposium on Algorithms and Computation (ISAAC 2012), ACM Symposium on the Theory of Computing (STOC 2014), International Cryptology Conference (CRYPTO 2015), International Conference on Cryptology and Information Security in Latin America (Latincrypt 2015), International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX 2015).
- Session chair: ITA (Information Theory and Applications Workshop) 2012 and 2013.

Invited Research Talks

- "Nearly Optimal Deterministic Algorithm for Sparse Walsh-Hadamard Transform". Invited talk at Case Western Reserve University (05/2015, hosted by Prof. Harold Connamacher).
- Invited talk at the 2015 Information Theory and Applications (ITA) Workshop, University of California, San Diego, CA (02/2015).
- 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).
- Invited talk at the 2014 Information Theory and Applications (ITA) Workshop, University of California, San Diego, CA (02/2014).
- "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), Case Western Reserve University (11/2014, hosted by Prof. Harold Connamacher).
- Invited talk at the 2013 Information Theory and Applications (ITA) Workshop, University of California, San Diego, CA (02/2013).
- "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 2012 Information Theory and Applications (ITA) Workshop, University of California, San Diego, CA (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 Theory and Combinatorial Group Testing". Invited talk at the 2011 Information Theory and Applications (ITA) Workshop, UC San Diego, CA (02/2011).
- "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 Projects Supervised

Student semester projects supervised at EPFL (2006–2010):

1. "Random Number Generator from Expanders" by Avinash Das Sahu. M.Sc. semester project, Winter semester, 2009.
2. "Turing Machine Emulator" by Ludovic Favre. B.Sc. semester project, Summer semester, 2009.
3. "Expander Codes" by Adrien Lücker. Mathematics fourth year semester project, Winter semester, 2008.
4. "Construction of Ramsey graphs" by Gaël Cotting. M.Sc. semester project, Winter semester, 2007.
5. "Poynomial Identity Testing" by Maged Thabet and Majdi Zahaf. B.Sc. semester project, Summer semester, 2007.
6. "Good Ensembles of Goppa Codes" by Ghid Maatouk. M.Sc. semester project, Winter semester, 2006.
7. "Primality Testing" by Kamal Tahiri Jouti. B.Sc. semester project, Summer semester, 2006.

Computer Skills

- Operating Systems: UNIX family, Microsoft Windows.
- Programming Languages/Environments:
  - Proficient in C++, C, Java, (Object) Pascal, LaTeX.
  - Familiar with Python, PHP, Javascript, HTML, SQL, Matlab.

References (in alphabetical order)

1. Anna Gál, Professor, Department of Computer Science, University of Texas at Austin, TX 78701, USA.
   email: `panni@cs.utexas.edu`, *phone:* +1(512)471-9539.
2. Venkatesan Guruswami, Professor, Computer Science Department, Carnegie Mellon University, Pittsburgh PA 15213, USA.
   email: `venkatg@cs.cmu.edu`, *phone:* +1(412)268-4899.
3. Johan Håstad, Professor, School of Computer Science and Communication (CSC), Royal Institute of Technology (KTH), Stockholm, Sweden.
   email: `johanh@csc.kth.se`, *phone:* +46(8)790-6289.
4. Piotr Indyk, Professor, MIT Computer Science and Artificial Intelligence Lab, Cambridge MA 02139, USA.
   email: `indyk@mit.edu`, *phone:* +1(617)452-3402.
5. 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.
6. Martin Vetterli, Professor, School of Computer and Communication Sciences (IC), Swiss Federal Institute of Technology, Lausanne, Switzerland.
   email: `martin.vetterli@epfl.ch`, *phone:* +41(21)693-5698.