Ragesh Jaiswal

PERSONAL INFORMATION

Address:
Department of Computer Science,
Columbia University,
1214 Amsterdam Avenue, New York, NY 10027-7003.

Voice: (858) 610-3119
E-mail: rjaiswal@cs.columbia.edu
WWW: www.cs.columbia.edu/~rjaiswal
Citizenship: India

RESEARCH INTERESTS

Algorithms, *Computational Complexity*, *Theoretical Cryptography.*

EDUCATION

- **PhD**, Computer Science and Engineering, UC San Diego, 2008.
  Advisor: Russell Impagliazzo.
  Thesis Title: New Proofs of (New) Direct Product Theorems.
- **M.Phil.**, Computer Science and Engineering, UC San Diego, 2006, GPA: 4.0/4.0.
- **MS**, Computer Science and Engineering, UC San Diego, 2005, GPA: 4.0/4.0.
- **B.Tech.**, Computer Science and Engineering, IIT Kanpur, 2003, GPA: 9.6/10.0.

EXPERIENCE

Postdoctoral Researcher, Columbia University, New York, October 2008 – Present.
Host: Rocco Servedio.

Research Assistant

- Research Assistant at University of California San Diego, USA (2003 – 2008).
- Visiting Students Research Program at Tata Institute of Fundamental Research, Bombay, India (May–June, 2002).

Teaching Assistant

- Teaching Assistant for undergraduate/graduate Algorithms and undergraduate Theory of Computation at University of California San Diego, USA (2003 – 2008).
- Co-Instructor for undergraduate level course on Data Structures and Algorithms at Indian Institute of Technology, Kanpur, India (May–June, 2003).

PUBLICATIONS

Journal Publications

- Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Avi Wigderson.: Uniform Direct Product Theorems: Simplified, Optimized and Derandomized. To appear in *SIAM Journal on Computing*.

- Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets.: Chernoff-type direct product theorems. *Journal of Cryptology*, 22: 75–92, 2009.

- Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets.: Approximately list-decoding direct product codes and uniform hardness amplification. *SIAM Journal on Computing*, Volume 39, Issue 2, pp. 564-605 (2009).

Conference Proceedings

- Nir Ailon, Ragesh Jaiswal, Claire Monteleoni.: Streaming k-means approximation. *To appear in Neural Information Processing Systems Conference (NIPS'09)*, 2009.

- Ilias Diakonikolas, Parikshit Gopalan, Ragesh Jaiswal, Rocco Servedio, Emanuele Viola.: Bounded independence fools halfspaces. *To appear in the Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS'09)*, 2009.

- Yevgeniy Dodis, Russell Impagliazzo, Ragesh Jaiswal, and Valentine Kabanets.: Security Amplification for Interactive Cryptographic Primitives. In *Theory of Cryptography Conference (TCC'09)*, pages 128–145, 2009.
  Invited to appear in *Journal of Cryptology.*

- Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Avi Wigderson.: Uniform Direct Product Theorems: Simplified, Optimized and Derandomized. *In Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC'08)*, pages 579–588, 2008.

- Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets.: Chernoff-type direct product theorems. *In Proceedings of the 27th Annual International Cryptology Conference (CRYPTO'07)*, pages 500–516, 2007.

- Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets.: Approximately list-decoding direct product codes and uniform hardness amplification. *In Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, pages 187–196, 2006.
  Invited to appear in *SIAM Journal on Computing* (FOCS special issue).

- Ritesh Kumar, Ragesh Jaiswal, Sanjeev K. Aggarwal.: An Inlining Technique in Jikes RVM to improve Performance. In *Proceedings of Advances in Computer Science and Technology*, St Thomas Virgin Islands, USA, pages 140-144, 2004.

- Ragesh Jaiswal, Pankaj Jalote, Kapil Narula, Vivek Pandey.: Case Study: Software Development of Personal Investment Management System. *An Integrated Approach to Software Engineering (Author: Pankaj Jalote), Springer, Third Edition.*

Talks

- Security Amplification for Interactive Cryptographic Primitives.
  - *Cryptography Seminar at New York University*, New York, February, 2009.
  - *6th Theory of Cryptography Conference (TCC'09)*, San Francisco, March, 2009.
- New Proofs of (New) Direct Product Theorems.
  - *China Theory Week 2008*, Tsinghua University, Beijing, China, September, 2008.
  - *CS Theory Seminar at Columbia University*, New York, November, 2008.
- Uniform Direct Product Theorems: Simplified, Optimized, and Derandomized.
  - *40th annual ACM symposium on Theory of Computing (STOC'08)*, Victoria, British Columbia, Canada, May, 2008.
  - *Workshop on Analytical Tools in Computational Complexity*, Banff International Research Station, Alberta, Canada, August, 2008.
  - *CS Theory Seminar at Microsoft Research India Lab*, India, October, 2008.
- Chernoff-Type Direct Product Theorems.
  - *27th Annual International Cryptology Conference (CRYPTO'07)*, Santa Barbara, CA, August, 2007.
  - *CS Theory Seminar at Princeton University*, Princeton, NJ, October 2007.
  - *CS Theory Seminar at University of Toronto*, Canada, March, 2008.
- Approximately list-decoding direct product codes and uniform hardness amplification.
  - *Workshop on Recent Advances in Computational Complexity*, Banff International Research Station, Alberta, Canada, August, 2006.
  - *47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, Berkeley, October, 2006.

Professional Service

- Reviewer for IEEE Symposium on Foundations of Computer Science (FOCS 2009), Theory of Cryptography Conference (TCC 2010).

ACADEMIC HONORS

- Fellowship awarded by UC San Diego for academic year 2003-2004.
- Award for academic excellence, IIT Kanpur, 1999 and 2000.
- Ranked 80^{th} in IIT-JEE-1999, the joint entrance examination for admission to the Indian Institutes of Technology (IIT).

COURSES

- Algorithms and Analysis, Advanced Algorithms, Computability and Complexity, Advanced Complexity, Lattice Algorithms, Modern Cryptography.
- Machine Learning, Computer Vision, Computer Architecture, Operating Systems, Database Theory, Compilers, Computer Networks, Distributed Systems.

LANGUAGES

- English, Hindi.