

Ragesh Jaiswal

PERSONAL INFORMATION

Address:
Department of Computer Science and Engineering,
University of California San Diego,
9500 Gilman Drive, La Jolla, CA 92093-0404.

Voice: (858) 610-3119
E-mail: rjaiswal@cs.ucsd.edu
WWW: www.cs.ucsd.edu/users/rjaiswal
Citizenship/Visa: Indian/F-1

RESEARCH INTERESTS

Derandomization, Cryptography, Computational Complexity and a more specific interest in *Hardness Amplification*.

EDUCATION

PhD. Candidate, University of California San Diego

Department of Computer Science and Engineering (2003 – present)
Expected graduation: June 2008.
Advisor: Prof. Russell Impagliazzo.

B. Tech., Indian Institute of Technology Kanpur, Kanpur, India

Bachelor's in Computer Science and Engineering (1999 – 2003)

ACADEMIC EXPERIENCE

Research

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

Teaching

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

PUBLISHED WORK

- **[IJK06]** Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets.: *Approximately list-decoding direct product codes and uniform hardness amplification*. In *FOCS 2006: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, pages 187–196. IEEE Computer Society, 2006. (Invited to the special issue of SIAM Journal on Computing (SICOMP)).

We describe an efficient randomized algorithm for approximate local list-decoding of direct product codes. As an application, we get *uniform* hardness amplification for $P^{NP_{\parallel}}$, the class of languages reducible to NP through one round of parallel oracle queries.

- **[IJK07]** Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets.: *Chernoff-type direct product theorems*. In *CRYPTO 2007: Proceedings of the 27th Annual International Cryptology Conference*, pages 500–516, 2007.

Consider a challenge-response protocol where the probability of a correct response is at least α for a legitimate user, and at most $\beta < \alpha$ for an attacker. One example is a CAPTCHA challenge, where a human should have a significantly higher chance of answering a single challenge (e.g., uncovering a distorted letter) than an attacker; another example is an argument system without perfect completeness. A natural approach to boost the gap between legitimate users and attackers is to issue many challenges, and accept if the response is correct for more than a threshold fraction, for the threshold chosen between α and β . We give the first proof that parallel repetition with thresholds improves the security of such protocols. We do this with a very general result about an attacker's ability to solve a large fraction of many independent instances of a hard problem, showing a Chernoff-like convergence of the fraction solved incorrectly to the probability of failure for a single instance.

- [IJKW08] Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Avi Wigderson.: *Uniform Direct Product Theorems: Simplified, Optimized and Derandomized. STOC 2008 (to appear)*. We simplify and improve the results of [IJK06] to get optimal list size for direct product codes. We also get a derandomized direct product theorem in the uniform setting.

WORKS IN
PROGRESS

- Russell Impagliazzo, Ragesh Jaiswal.: *A $2^{n/6}$ -time algorithm for maximum independent set for graphs of bounded degree 3*. We study properties exhibited by graphs with bounded degree 3 in the context of the Maximum Independent Set problem and use them to improve upon the previous best algorithm.
- Russell Impagliazzo, Ragesh Jaiswal.: *General conditions for rapid convergence of metropolis on hierarchical markov chains*. We give general sufficient conditions for uniform rapid convergence of the Metropolis algorithm at all temperatures, on hierarchical search graphs (where edges are between solutions of same or consecutive integer values). Such problems include graph matching and independent set. Our conditions generalize results of Jerrum and Sinclair showing rapid convergence for Metropolis on the chain of matchings of dense graphs.
- Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Bruce M. Kapron, Valerie King.: *Security Amplification for Channels with Memory*. We propose a very general model of channel with state, that makes fewer assumptions about the way the channel is constructed or the computational resources of the users and attackers. In this abstract setting, we consider the general problem of amplifying the gap between an attacker's ability to break the channel and a legitimate user's ability to make use of the channel.

TALKS

- 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.
- Approximately list-decoding direct product codes and uniform hardness amplification. *47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, Berkeley, USA, October, 2006.
- Chernoff-Type Direct Product Theorems. *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August, 2007.
- Chernoff-Type Direct Product Theorems. *CS Theory Seminar at Princeton University*, Princeton, NJ, USA, October 2007.

REFERENCES

Russell Impagliazzo

Dept. of Computer Science and Engineering,
University of California San Diego, USA.

Email: russell@cs.ucsd.edu

Phone: (609) 734-8029

Valentine Kabanets

Computing Science,
Simon Fraser University, Canada.

Email: kabanets@cs.sfu.ca

Phone: +1 778 782 6912

Daniele Micciancio

Dep. of Computer Science and Engineering,
University of California San Diego, USA.

Email: daniele@cs.ucsd.edu

Phone: (858) 822-2577