

Sergey Yekhanin

Curriculum Vitae
September 11, 2007

School of Mathematics,
Institute for Advanced Study
1 Einstein Drive, Princeton NJ 08540
Homepage: <http://math.ias.edu/~yekhanin>

Office tel.: (609) 734-8188
Home tel.: (609) 279-2824
Citizenship: Russian
E-mail: yekhanin@ias.edu

Research Interests

Complexity theory, Cryptography, Error-correcting codes.

Current Position

Member of School of Mathematics.
9/2006 – present Institute for Advanced Study, Princeton, NJ 08540.

Education

Ph.D. in Computer Science.

2003-2007 *Massachusetts Institute of Technology*, Cambridge, MA, USA.
Thesis advisor: Prof. Madhu Sudan.
Areas of research: Complexity theory and Cryptography.
Ph.D. thesis title: *Locally Decodable Codes and Private Information Retrieval Schemes*.

Diploma in Computer Science, 2002

1997-2002 *Moscow State University*, Moscow, Russia.
Thesis advisor: Prof. Alexander Petrenko.
Area of research: formal methods.

Honors:

- MIT George M. Sprows Award for the best doctoral theses in Computer Science, 2007.
- Best Paper Award - 2007 ACM Symposium on the Theory of Computing (STOC).
- Best Student Paper Award - 2007 ACM Symposium on the Theory of Computing (STOC).
- MIT Presidential Fellow: 2003.
- Diploma with Honors from Moscow State University: 2002.
- Soros Mathematical Fellow: 1999.

Teaching Experience:

- *Introduction to Algorithms*, MIT, 2006.

- *Advanced Algorithms*, MIT, 2005.
- *Advanced Complexity Theory*, MIT, 2004.

Work Experience:

5-8 / 2006	Microsoft Research, Silicon Valley Campus Summer Intern
5-8 / 2005	Mitsubishi Electric Research Laboratory Summer Intern
2001-2002	Parascript, LLC Research programmer
1999-2001	Procter and Gamble corporation Systems engineer

Publications:

1. Kiran Kedlaya, Sergey Yekhanin
"Locally Decodable Codes from Nice Subsets of Finite Fields and Prime Factors of Mersenne Numbers"
 Electronic Colloquium on Computational Complexity, TR07-040, 2007.
2. Sergey Yekhanin
"Towards 3-Query Locally Decodable Codes of Subexponential Length"
 Proc. of the 39th ACM Symposium on Theory of Computing (STOC), pp. 266-274, 2007.
3. Alexander Razborov, Sergey Yekhanin
"An $\Omega(n^{1/3})$ Lower Bound for Bilinear Group Based Private Information Retrieval"
 Proc. of the 47th Symp. on Foundations of Computer Science (FOCS), pp. 739-748, 2006.
4. Nicholas Harvey, Mihai Patrascu, Yonggang Wen, Sergey Yekhanin, Vincent W. S. Chan
"Non-Adaptive Fault Diagnosis for All-Optical Networks via Combinatorial Group Testing on Graphs"
 Proc. of the 26th IEEE Conference on Computer Communications (INFOCOM), 2007.
5. Nicholas Harvey, David Karger, Sergey Yekhanin
"On The Hardness of Matrix Completion"
 Proc. of ACM-SIAM Symposium on Discrete Algorithms (SODA), pp.1103-1111, 2006.
6. David Woodruff, Sergey Yekhanin
"A Geometric Approach to Information Theoretic Private Information Retrieval"
 Proc. of the 20th IEEE Computational Complexity Conference (CCC), pp. 275-284, 2005.

7. Sergey Yekhanin
"A Note on Plane Pointless Curves"
Finite Fields and Their Applications, vol. 13, Issue 2, pp. 418-422, 2007.
8. Sergey Yekhanin, Ilya Dumer
"Long Nonbinary Codes Exceeding the Gilbert - Varshamov Bound for any Fixed Distance"
IEEE Transactions on Information Theory, vol. 50, Issue 10, pp. 2357-2362, 2004.
9. Sergey Yekhanin
"Improved Upper Bound for the Redundancy of Fix-Free Codes"
IEEE Transactions on Information Theory, vol. 50, Issue 11, pp. 2815-2818, 2004.
10. Emin Martinian, Sergey Yekhanin, Jonathan S. Yedidia
"Secure Biometrics Via Syndromes"
In Proc. of the Allerton Conference on Communication, Control, and Computing, 2005.
11. Arkadii D'yachkov, Vyacheslav Rykov, David Torney, Sergey Yekhanin
"On Application of the partition distance concept to a comparative analysis of psychological or sociological tests"
Stochastic Analysis and Applications, vol. 24, pp. 61-78, 2006.
12. Anthony J. Macula, Vyacheslav Rykov, Sergey Yekhanin
"Trivial Two-Stage Group Testing for Complexes Using Almost Disjunct Matrices"
Discrete and Applied Mathematics, vol. 137, pp. 97-107, 2004.
13. Arkadii D'yachkov, Pavel Vilenkin, Sergey Yekhanin
"Upper Bound on the Rate of Superimposed (s,l) codes based on Engel's Inequality"
Proc. of Intern. Conf. on Algebraic and Combin. Coding Theory (ACCT), pp. 95-99, 2002.
14. Sergey Yekhanin
"Sufficient Conditions of Existence of Fix-Free Codes"
Proc. of International Symposium on Information Theory (ISIT), p. 284, 2001.
15. Arkadii D'yachkov, Vladimir Lebedev, Pavel Vilenkin, Sergey Yekhanin
"Cover-Free Families and Superimposed Codes: Constructions, Bounds and Applications to Cryptography and Group Testing"
Proc. of International Symposium on Information Theory (ISIT), p. 117, 2001.
16. Arkadii D'yachkov, Anthony Macula, David Torney, Pavel Vilenkin, Sergey Yekhanin
"New Results in the Theory of Superimposed Codes"
Proc. of Intern. Conf. on Algebraic and Combin. Coding Theory (ACCT), pp. 126-136, 2000.
17. Sergey Yekhanin, Anna Kochetova
"Evaluation of Estimates for Standard Learning Information in Pattern Recognition Problems"
Computational Mathematics and Mathematical Physics, vol. 42, N3, pp. 419-423, 2002.
18. Sergey Yekhanin
"Some New Constructions of Optimal Superimposed Designs"
Proc. of Intern. Conf. on Algebraic and Combin. Coding Theory (ACCT), pp. 232-235, 1998.

Invited Talks:

- *Long Nonbinary Codes Exceeding the Gilbert - Varshamov Bound for any Fixed Distance*
Allerton Conference on Communication, Control, and Computing, October 2004.
- *New Locally Decodable Codes and Private Information Retrieval Schemes*
IPAM workshop: “Securing cyberspace: Applications and Foundations of Cryptography and Computer Security”, October 2006.
- *An $\Omega(n^{1/3})$ Lower Bound for Bilinear Group Based Private Information Retrieval*
IPAM workshop: “Securing cyberspace: Applications and Foundations of Cryptography and Computer Security”, October 2006.
- *New Locally Decodable Codes and Private Information Retrieval Schemes*
IAS, Theoretical Computer Science / Discrete Mathematics Seminar, November 2006.
- *New Locally Decodable Codes and Private Information Retrieval Schemes*
Northeastern University, College of Comp. and Inform. Science Colloquia, February 2007.
- *New Locally Decodable Codes and Private Information Retrieval Schemes*
University of Connecticut, Departmental Colloquium, March 2007.
- *New Locally Decodable Codes and Private Information Retrieval Schemes*
Harvard, Theory of Computation Seminar, April 2007.
- *Locally Decodable Codes*
Berkeley, Theory Lunch, April 2007.
- *Towards 3-Query Locally Decodable Codes of Subexponential Length*
Oberwolfach Workshop on Complexity Theory, June 2007.
- *New Locally Decodable Codes and Private Information Retrieval Schemes*
Georgia Inst. of Tech., Algorithms and Randomness Center, Colloquium, September 2007.

Journal Refereeing:

- SIAM Journal of Computing
- IEEE Transactions on Information Theory
- IEEE Signal Processing Letters

References:

Prof. Madhu Sudan
Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

Cambridge, MA, 02139

madhu@mit.edu

Prof. Alexander A. Razborov

School of Mathematics

Institute for Advanced Study

Princeton, NJ, 08540

razborov@math.ias.edu

Prof. Oded Goldreich

Faculty of Mathematics and Computer Science

Weizmann Institute of Science

Rehovot, Israel

oded.goldreich@weizmann.ac.il

Prof. Ilya Dumer

Electrical Engineering Department

College of Engineering

University of California, Riverside

Riverside, CA, 92521-0429

dumer@ee.ucr.edu