Alexander Golovnev

☎ (917) 251-0235
✉ golovnev@cims.nyu.edu
cims.nyu.edu/~golovnev/

Present Occupation

2017–present **Columbia University**, *New York, USA*.
Research Scientist, Computer Science Department.

2017–present **Yahoo Research**, *New York, USA*.
Research Scientist.

Education

2012–2017 **New York University**, *New York, USA*.
Ph.D., Computer Science Department.
- Thesis: "Circuit Complexity: New Techniques and Their Limitations".
- Advisors: Oded Regev, Yevgeniy Dodis.

2010–2012 **St. Petersburg Academic University of the Russian Academy of Sciences**, *St. Petersburg, Russia*.
M.Sc., Department of Information and Mathematics Technologies, Diploma with Honors.
- Thesis: "Approximation Algorithms for Traveling Salesman and Shortest Superstring Problems".
- Advisor: Alexander S. Kulikov.

2005–2010 **Belarusian State University**, *Minsk, Belarus*.
Specialist (M.Sc.), Department of Applied Mathematics and Informatics, Diploma with Honors.
- Thesis: "Efficient Algorithms for Vector Fonts Conversion".
- Advisor: Stanislav L. Sobolevskiy.

2008–2010 **Belarusian State Conservatory**, *Minsk, Belarus*.
Opera Singing Department.

2009–2010 **Belarusian State University**, *Minsk, Belarus*.
Faculty of Education, Diploma with Honors.

Research interests

Algorithms, Computational Complexity, Cryptography.

Summer Internships

2016 Summer internship at Stanford University, host: Ryan Williams.

2015 Summer internship at Tel Aviv University, host: Iftach Haitner.

2014 Summer internship at Saint Petersburg Department of the Russian Academy of Sciences, host: Alexander Kulikov.

2013 Summer internship at Institute of Science and Technology in Austria, host: Krzysztof Pietrzak.

Honors and awards

2016 Best young researcher award (by St. Petersburg department of the Russian Academy of Sciences).

2012 IPEC excellent student paper award.

2003–2005 National Olympiads in Informatics. 1st degree diploma.

2002–2006 National conferences in Mathematics. 1st degree diploma.

2002–2006 National conferences in Informatics. 1st degree diploma.

2003–2005 International mathematical competition Tournament of the Towns. 1st degree diploma.

2002–2006 North-Eastern European Regional Contests (ACM NEERC). 2nd degree diploma.

Research Fellowships

2012–2017 Henry MacCracken fellowship.

2010–2011 Yandex's personal research fellowship.

2003, 04, 05 The President's fellowhips for young scientists.

Teaching

2017 Selected Topics in Circuit Complexity, CS Center. St. Petersburg, Russia.

2017 Coursera Course on Graph Theory.

2016 Teaching Assistant, Graduate course on Algorithms, NYU. *Homework sets, recitations, office hours, grading.* New York, NY.

2016 Tutor, Graduate course on Random Graphs. New York, NY.

2014 Teaching Assistant, Advanced Algorithms. Minsk, Belarus.

2013 Teaching Assistant, .Net. Minsk, Belarus.

2008–2010 Teaching Assistant, Algorithms. Minsk, Belarus.

Service

2012 Assistant organizer of Joint Advanced Student School (JASS 2012).

2011 Assistant organizer of International CS Symposium in Russia (CSR 2011).

2010 Chair of Minsk .Net School.

2010 Chair of Hrodna .Net School.

Reviewer STOC, FOCS, SODA, CRYPTO, Eurocrypt, STACS, ITCS, TCC, CSR, SOFSEM, WADS, IPEC, PKC, Theory Comput, Algorithmica, SIDMA, Discrete Math, IPL, Theor Comput Sci, J. Comput Syst Sci, Ars Comb, J. Comp Math, MSc Thesis.

Technical skills

C#, Java (Sun Certified Programmer), C/C++, OOP, Algorithms.

Industrial Experience

2012 Project Manager, Senior Developer. Altsoft. Minsk, Belarus.

2005–2010 Team Leader, Senior Developer. Altsoft. Minsk, Belarus.

Publications

[1] A. Golovnev, D. Reichman, and I. Shinkar. Detecting patterns can be hard: Circuit lower bounds for the pattern matching problem. *arXiv preprint arXiv:1709.02034*, 2017.

[2] H. Bennett, A. Golovnev, and N. Stephens-Davidowitz. On the quantitative hardness

of CVP. In *Foundations of Computer Science (FOCS)*. IEEE, 2017.

[3] A. Golovnev, O. Regev, and O. Weinstein. The minrank of random graphs. In *Approximation, Randomization, and Combinatorial Optimization (RANDOM)*. LIPIcs, 2017.

[4] M. Cygan, F. V. Fomin, A. Golovnev, A. S. Kulikov, I. Mihajlin, J. Pachocki, and A. Socała. Tight lower bounds on graph embedding problems. *Journal of the ACM (JACM)*, 64(3):18, 2017.

[5] M. G. Find, A. Golovnev, E. A. Hirsch, and A. S. Kulikov. A better-than-3n lower bound for the circuit complexity of an explicit function. In *Foundations of Computer Science (FOCS)*. IEEE, 2016.

[6] M. Cygan, F. V. Fomin, A. Golovnev, A. S. Kulikov, I. Mihajlin, J. Pachocki, and A. Socała. Tight bounds for graph homomorphism and subgraph isomorphism. In *ACM-SIAM Symposium on Discrete Algorithms (SODA)*. SIAM, 2016.

[7] A. Golovnev and A. S. Kulikov. Weighted gate elimination: Boolean dispersers for quadratic varieties imply improved circuit lower bounds. In *7th Innovations in Theoretical Computer Science Conference (ITCS)*. ACM, 2016.

[8] A. Golovnev, A. S. Kulikov, and I. Mihajlin. Families with infants: Speeding up algorithms for NP-hard problems using FFT. *ACM Trans. Algorithms (TALG)*, 12(3):35:1–35:17, 2016.

[9] A. Golovnev, E. A. Hirsch, A. Knop, and A. S. Kulikov. On the limits of gate elimination. In *Mathematical Foundations of Computer Science (MFCS)*. LIPIcs, 2016.

[10] A. Golovnev, A. S. Kulikov, A.V. Smal, and S. Tamaki. Circuit size lower bounds and #SAT upper bounds through a general framework. In *Mathematical Foundations of Computer Science (MFCS)*. LIPIcs, 2016.

[11] Y. Dodis, C. Ganesh, A. Golovnev, A. Juels, and T. Ristenpart. A formal treatment of backdoored pseudorandom generators. In *Advances in Cryptology (EUROCRYPT)*. Springer, 2015.

[12] M. Skorski, A. Golovnev, and K. Pietrzak. Condensed unpredictability. In *Automata, Languages, and Programming (ICALP)*, volume 1. Springer, 2015.

[13] F. V. Fomin, A. Golovnev, A. S. Kulikov, and I. Mihajlin. Lower bounds for the graph homomorphism problem. In *Automata, Languages, and Programming (ICALP)*, volume 1. Springer, 2015.

[14] D. Aggarwal and A. Golovnev. A note on lower bounds for non-interactive message authentication using weak keys. In *Information Theory Workshop (ITW)*. IEEE, 2015.

[15] A. Golovnev, A. S. Kulikov, and I. Mihajlin. Families with infants: a general approach to solve hard partition problems. In *Automata, Languages, and Programming (ICALP)*, volume 1. Springer, 2014.

[16] A. Golovnev and K. Kutzkov. New exact algorithms for the 2-constraint satisfaction problem. *Theoretical Computer Science (TCS)*, 526:18–27, 2014.

[17] A. Golovnev, A. S. Kulikov, and I. Mihajlin. Solving SCS for bounded length strings in fewer than 2^n steps. *Information Processing Letters (IPL)*, 114(8):421–425, 2014.

[18] A. Golovnev. Approximating asymmetric TSP in exponential time. *International Journal of Foundations of Computer Science (IJFCS)*, 25(01):89–99, 2014.

[19] A. Golovnev, A. S. Kulikov, and I. Mihajlin. Solving 3-superstring in $3^{n/3}$ time. In *Mathematical Foundations of Computer Science (MFCS)*. Springer, 2013.

[20] A. Golovnev, A. S. Kulikov, and I. Mihajlin. Approximating shortest superstring problem using de bruijn graphs. In *Combinatorial Pattern Matching (CPM)*. Springer, 2013.

[21] I. Bliznets and A. Golovnev. A new algorithm for parameterized MAX-SAT. In *Parameterized and Exact Computation (IPEC)*. Springer, 2012.

[22] A. Golovnev. New upper bounds for MAX-2-SAT and MAX-2-CSP w.r.t. the average variable degree. In *Parameterized and Exact Computation (IPEC)*. Springer, 2012.