Alexander Golovnev

alex.golovnev@gmail.com
golovnev.org

Research interests

Computational Complexity, Algorithms, Cryptography, Learning Theory.

Employment

2020–present **Georgetown University**.
Assistant Professor, Computer Science Department.

2023–present **National University of Singapore**.
Visiting Professor, Centre for Quantum Technologies.

2018–2020 **Harvard University**.
Rabin Postdoctoral Fellow, Theory of Computing Group.

2017–2018 **Columbia University**.
Postdoctoral Fellow, Computer Science Department.

2017–2018 **Yahoo Research**.
Research Scientist.

Education

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

2012–2015 **Belarusian Academy of Sciences**.
Ph.D., Discrete Mathematics.
- Thesis: "Efficient Exponential-Time Algorithms for Combinatorial Problems".
- Advisor: Alexander N. Kurbatskiy.

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

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

Honors and awards

2024 NSF CAREER Award.

2023 Paper [8] in TALG special issue for SODA 2023.

2020 Paper [25] in SICOMP special issue for FOCS 2020.

2018–2020 Rabin Postdoctoral Fellowship.

2016 Best young researcher award (by St. Petersburg dept. of the Russian Academy of Sci).

2012–2017 Henry MacCracken fellowship.

2012 IPEC excellent student paper award.

2010–2011 Yandex's personal research fellowship.

2003–2005 Annual President's fellowhips for young scientists.

2002–2005 National Olympiads/Conferences in Informatics/Mathematics. 1st degree diplomas.

Students

2020–present Sidhant Saraogi (joint with Justin Thaler).

2021–present Karthik Gajulapalli.

2021–present Samuel King.

2021–present Satyajeet Nagargoje (M.Sc. 2021–2023; Ph.D. 2023–present).

Teaching

2024 *Introduction to Algorithms.*
Georgetown University

2021,2023 *Gems of Theoretical Computer Science.*
Georgetown University

2021,2022 *Graduate Gems of Theoretical Computer Science.*
Georgetown University

2020 *Matrix Rigidity.*
Georgetown University

2018 *On Problems as Hard as Satisfiability.*
Summer school on Recent Advances in Algorithms

2017 *Selected Topics in Circuit Complexity.*
Mini course, Computer Science Center

2017–present *Specialization on Discrete Math.*
5 Courses taught through Coursera (together with 4 other instructors).

2014 *Advanced Algorithms.*

2013 *.Net.*

2008–2010 *Algorithms.*

Service

PC member for CSR 2022, FOCS 2022, STOC 2024, CCC 2024.

2022 Organizer of the workshop on Fine-Grained Cryptography at FSTTCS 2022.

2020 Organizer of the workshop on Matrix Rigidity at FSTTCS 2020.

2022-2023 Associate Editor for SICOMP's special edition for FOCS 2022.

2017-present Co-creator of a 5-course specialization on Discrete Math through Coursera

2021-present Organizer of the Georgetown Theory Seminar.

2020-present Organizer of the Georgetown CS Colloquium.

2019-2020 Organizer of the Harvard Theory Seminar.

2017-2018 Organizer of the Yahoo Research Seminar.

2015 Organizer of the NYU Student Seminar.

2012 Co-organizer of Joint Advanced Student School (JASS 2012).

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

2010 Chair of "Minsk .Net School" and "Hrodna .Net School".

Publications

[1] E. Chung, A. Golovnev, Z. Li, M. Obremski, S. Saraogi, and N. Stephens-Davidowitz. The hardness of range avoidance for randomized algorithms implies minicrypt, 2024. Manuscript.

[2] C.-N. Chou, A. Golovnev, M. Sudan, and S. Velusamy. Sketching approximability of all finite csps. *Journal of the ACM (JACM)*, 2024.

[3] V. Asadi, A. Golovnev, T. Gur, I. Shinkar, and S. Subramanian. Quantum worst-case to average-case reductions for all linear problems. In *SODA*, 2024. Prelim. version in QIP 2023.

[4] K. Gajulapalli, A. Golovnev, and S. King. On the power of adaptivity for function inversion. In *ITC*, 2024.

[5] A. Golovnev, Z. Guo, P. Hatami, S. Nagargoje, and C. Yan. Hilbert functions and low-degree randomness extractors. In *RANDOM*, 2024.

[6] H. Bennett, K. Gajulapalli, A. Golovnev, and E. Warton. Matrix multiplication verification using coding theory. In *RANDOM*, 2024.

[7] D. Aggarwal, H. Bennett, Z. Brakerski, A. Golovnev, R. Kumar, Z. Li, S. Peters, N. Stephens-Davidowitz, and V. Vaikuntanathan. Lattice problems beyond polynomial time. In *STOC*, 2023.

[8] T. Belova, A. Golovnev, A. S. Kulikov, I. Mihajlin, and D. Sharipov. Polynomial formulations as a barrier for reduction-based hardness proofs. In *SODA*, 2023. Invited to the TALG Special Issue.

[9] A. Golovnev, T. Gur, and I. Shinkar. Derandomization of cell sampling. In *SOSA*, 2023.

[10] A. Golovnev, S. Guo, S. Peters, and N. Stephens-Davidowitz. Revisiting time-space tradeoffs for function inversion. In *CRYPTO*, 2023.

[11] A. Golovnev, J. Lee, S. Setty, J. Thaler, and R. S. Wahby. Brakedown: Linear-time and field-agnostic SNARKs for R1CS. In *CRYPTO*, 2023.

[12] K. Gajulapalli, A. Golovnev, S. Nagargoje, and S. Saraogi. Range avoidance for constant-depth circuits: Hardness and algorithms. In *RANDOM*, 2023.

[13] A. Golovnev, S. Guo, S. Peters, and N. Stephens-Davidowitz. The (im)possibility of simple search-to-decision reductions for approximate optimization. In *APPROX*, 2023.

[14] M. G. Find, A. Golovnev, E. A. Hirsch, and A. S. Kulikov. Improving $3n$ circuit complexity lower bounds. *Computational Complexity*, 2023.

[15] C.-N. Chou, A. Golovnev, M. Sudan, A. Velingker, and S. Velusamy. Linear space streaming lower bounds for approximating CSPs. In *STOC*, 2022.

[16] V. Asadi, A. Golovnev, T. Gur, and I. Shinkar. Worst-case to average-case reductions via additive combinatorics. In *STOC*, 2022.

[17] C.-N. Chou, A. Golovnev, A. Shahrasbi, M. Sudan, and S. Velusamy. Sketching approximability of (weak) monarchy predicates. In *APPROX*, 2022.

[18] A. Golovnev, G. Posobin, O. Regev, and O. Weinstein. Polynomial data structure lower bounds in the group model. *SIAM Journal on Computing (SICOMP)*, (1), 2022.

[19] A. Golovnev and I. Haviv. The (generalized) orthogonality dimension of (generalized) Kneser graphs: Bounds and applications. *Theory of Computing (ToC)*, 18(1):1–22, 2022.

[20] C.-N. Chou, A. Golovnev, M. Sudan, and S. Velusamy. Approximability of all finite CSPs in the dynamic streaming setting. In *FOCS*, 2021.

[21] D. Aggarwal, H. Bennett, A. Golovnev, and N. Stephens-Davidowitz. Fine-grained hardness of CVP(P)—Everything that we can prove (and nothing else). In *SODA*, 2021.

[22] A. Golovnev and I. Haviv. The (generalized) orthogonality dimension of (generalized) Kneser graphs: Bounds and applications. In *CCC*, 2021.

[23] A. Golovnev, A. Kulikov, and R. Williams. Circuit depth reductions. In *ITCS*, 2021.

[24] A. Golovnev, A. Kulikov, V. Podolskii, and A. Shen. *Discrete Mathematics for Computer Science*. LeanPub, 2021.

[25] A. Golovnev, G. Posobin, O. Regev, and O. Weinstein. Polynomial data structure lower bounds in the group model. In *FOCS*, 2020. Invited to the SICOMP Special Issue.

[26] C.-N. Chou, A. Golovnev, and S. Velusamy. Optimal streaming approximations for all boolean Max-2CSPs and Max-kSAT. In *FOCS*, 2020.

[27] A. Golovnev, S. Guo, T. Horel, S. Park, and V. Vaikuntanathan. Data structures meet cryptography: 3SUM with preprocessing. In *STOC*, 2020.

[28] P. Gaudry and A. Golovnev. Breaking the encryption scheme of the Moscow internet voting system. In *FC*, 2020.

[29] Z. Dvir, A. Golovnev, and O. Weinstein. Static data structure lower bounds imply rigidity. In *STOC*, 2019.

[30] A. Golovnev, D. Pál, and B. Szörényi. The information-theoretic value of unlabeled data in semi-supervised learning. In *ICML*, 2019.

[31] A. Golovnev, R. Ilango, R. Impagliazzo, V. Kabanets, A. Kolokolova, and A. Tal. $\mathrm{AC}^0[p]$ lower bounds against MCSP via the coin problem. In *ICALP*, 2019.

[32] A. Golovnev, M. Göös, D. Reichman, and I. Shinkar. String matching: Communication, circuits, and learning. In *RANDOM*, 2019.

[33] A. Golovnev, A. Kulikov, A. Logunov, I. Mihajlin, and M. Nikolaev. Collapsing superstring conjecture. In *APPROX*, 2019.

[34] A. Golovnev, E. Hirsch, A. Knop, and A. Kulikov. On the limits of gate elimination. *Journal of Computer and System Sciences (JCSS)*, 96:107–119, 2018.

[35] A. Golovnev, O. Regev, and O. Weinstein. The minrank of random graphs. *IEEE Transactions on Information Theory (ToIT)*, 64(11):6990–6995, 2018.

[36] A. Golovnev, A. Kulikov, A. Smal, and S. Tamaki. Gate elimination: Circuit size lower bounds and #SAT upper bounds. *Theoretical Computer Science (TCS)*, 719:46–63, 2018.

[37] 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.

[38] H. Bennett, A. Golovnev, and N. Stephens-Davidowitz. On the quantitative hardness of CVP. In *FOCS*, 2017.

[39] A. Golovnev, O. Regev, and O. Weinstein. The minrank of random graphs. In *RANDOM*, 2017.

[40] 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 *FOCS*, 2016.

[41] 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 *SODA*, 2016.

[42] A. Golovnev and A. S. Kulikov. Weighted gate elimination: Boolean dispersers for quadratic varieties imply improved circuit lower bounds. In *ITCS*, 2016.

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

[44] A. Golovnev, E. A. Hirsch, A. Knop, and A. S. Kulikov. On the limits of gate elimination. In *MFCS*, 2016.

[45] A. Golovnev, A. S. Kulikov, A.V. Smal, and S. Tamaki. Circuit size lower bounds and #SAT upper bounds through a general framework. In *MFCS*, 2016.

[46] Y. Dodis, C. Ganesh, A. Golovnev, A. Juels, and T. Ristenpart. A formal treatment of backdoored pseudorandom generators. In *EUROCRYPT*, 2015.

[47] M. Skorski, A. Golovnev, and K. Pietrzak. Condensed unpredictability. In *ICALP*, 2015.

[48] F. V. Fomin, A. Golovnev, A. S. Kulikov, and I. Mihajlin. Lower bounds for the graph homomorphism problem. In *ICALP*, 2015.

[49] D. Aggarwal and A. Golovnev. A note on lower bounds for non-interactive message authentication using weak keys. In *ITW*, 2015.

[50] A. Golovnev, A. S. Kulikov, and I. Mihajlin. Families with infants: a general approach to solve hard partition problems. In *ICALP*, 2014.

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

[52] 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.

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

[54] A. Golovnev, A. S. Kulikov, and I. Mihajlin. Solving 3-superstring in $3^{n/3}$ time. In *MFCS*, 2013.

[55] A. Golovnev, A. S. Kulikov, and I. Mihajlin. Approximating shortest superstring problem using de Bruijn graphs. In *CPM*, 2013.

[56] I. Bliznets and A. Golovnev. A new algorithm for parameterized MAX-SAT. In *IPEC*, 2012. Excellent Student Paper Award.

[57] A. Golovnev. New upper bounds for MAX-2-SAT and MAX-2-CSP w.r.t. the average variable degree. In *IPEC*, 2012.

[58] H. Chen, A. Golovnev, and D. Pál. Detecting phishing emails. Technical report, TechPulse, 2018.

[59] T. Dick, A. Golovnev, and D. Pál. Fighting spam with nearest neighbor and clustering. Technical report, Yahoo Research, 2018.

Research Visits

2022,2023, 2024 Visiting Professor at National University of Singapore, host: Divesh Aggarwal.

2016 Research intern at Stanford University, host: Ryan Williams.

2015 Research intern at Tel Aviv University, host: Iftach Haitner.

2014 Research intern at the Russian Academy of Sciences, host: Alexander Kulikov.

2013 Research intern at IST Austria, host: Krzysztof Pietrzak.

Miscellaneous

Programming Java, C#, C++, Python.

2008-2010 Graduated from Opera Singing Department of Belarusian State Conservatory.

2009-2010 Degree in Education from Belarusian State University, Diploma with Honors.

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

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

2005–2007 Folk Rock band in Minsk, Belarus.