Oleg Zaikin

Curriculum Vitae

✉ *oleg.zaikin@icc.ru*
Leading researcher at
ISDCT SB RAS

Research interests

Satisfiability; Cryptanalysis; Combinatorics; Black-box optimization; Parallel computing

Education

2009 **PhD in Computer Science**, *Tomsk State university*, Tomsk, Russia.
Title: "A parallel SAT solving technology and its implementation in the form of a package of applied programs"
Advisor: Alexander Semenov

2005 **MSc in Mathematics**, *Irkutsk State University*, Irkutsk, Russia.
Title: "Heuristic algorithms for finding satisfying assignments of satisfiable CNFs"
Advisor: Alexander Semenov

Experience

Research

2022–date **Leading researcher**, *Matrosov Institute for System Dynamics and Control Theory SB RAS, Laboratory of Logical and Optimization Methods for Complex Systems Analysis*, Irkutsk, Russia.

2020–2022 **Research assistant**, *Swansea University, Department of Computer Science, Theoretical Computer Science research group*, Swansea, United Kingdom.

2019–2020 **Leading researcher**, *Matrosov Institute for System Dynamics and Control Theory SB RAS, Laboratory of Logical and Optimization Methods for Complex Systems Analysis*, Irkutsk, Russia.

2018–2019 **Postdoctoral researcher**, *ITMO University, eScience Research Institute*, Saint Petersburg, Russia.

2017–2018 **Senior researcher**, *Matrosov Institute for System Dynamics and Control Theory SB RAS, Laboratory of Logical and Optimization Methods for Complex Systems Analysis*, Irkutsk, Russia.

2016 **Postdoctoral researcher**, *Dorodnicyn Computing Centre RAS, Department of Applied Optimization Problems*, Moscow, Russia.

2011–2016 **Researcher**, *Matrosov Institute for System Dynamics and Control Theory SB RAS, Laboratory of Discrete Analysis and Applied Logic*, Irkutsk, Russia.

2009–2010 **Junior researcher**, *Matrosov Institute for System Dynamics and Control Theory SB RAS, Laboratory of Discrete Analysis and Applied Logic*, Irkutsk, Russia.

2005–2008 **PhD student**, *Matrosov Institute for System Dynamics and Control Theory SB RAS, Laboratory of Discrete Analysis and Applied Logic*, Irkutsk, Russia.

Teaching

2024 **Associate professor**, *Matrosov Institute for System Dynamics and Control Theory SB RAS*, Irkutsk, Russia.
Courses taught:
- Mathematical foundation of computer science, autumn 2024

2020 **Assistant professor**, *Matrosov Institute for System Dynamics and Control Theory SB RAS*, Irkutsk, Russia.
Courses taught:
- Introduction to mathematical modelling, spring 2020

2018–2019 **Assistant professor**, *ITMO University*, Saint Petersburg, Russia.
Courses taught:
- Algorithms design and analysis, autumn 2018
- Machine learning technologies, spring 2019

2018 **Guest professor**, *Far Eastern Federal University*, Vladivostok, Russia.
Courses taught:
- Applying machine learning to geoacoustic inversion problems, summer 2018

2017 **Guest professor**, *Far Eastern Federal University*, Vladivostok, Russia.
Courses taught:
- Applying volunteer computing to hard scientific problems, summer 2017

2009–2016 **Assistant professor**, *Irkutsk State University*, Irkutsk, Russia.
Courses taught:
- Introduction to computer science, autumn 2009 – spring 2012
- Introduction to algorithms and data structures, autumn 2012 – spring 2014
- Modern computational technologies, autumn 2013 – spring 2014
- Program and data security, autumn 2015 – winter 2016

Awards

2019 MapleLCMDistChronoBT-DL is one of the best SAT solvers at SAT Race 2019 (1st in the UNSAT and SAT+UNSAT tracks, 2nd in the SAT track).

Publication activity

Google scholar 81 publications, h-index 17

Scopus 58 publications, h-index 10

Main publications

2024a O. Zaikin. "Inverting Cryptographic Hash Functions via Cube-and-Conquer". *Journal of Artificial Intelligence Research*. (2024)

2024b O. Zaikin. "Inverting step-reduced SHA-1 and MD5 by parameterized SAT solvers". In *Proc. 30th International Conference on Principles and Practice of Constraint Programming*. (2024)

2022a O. Zaikin. "Inverting 43-step MD4 via Cube-and-Conquer". In *Proc. 31st International Joint Conference On Artificial Intelligence (IJCAI-ECAI'2022)*. (2022)

2021a O. Kullmann, O. Zaikin. "Projection heuristics for binary branchings between sum and product". In *Proc. 24th International Conference on Theory and Applications of Satisfiability Testing (SAT'2021)*. (2021)

2021b A. Semenov, O. Zaikin., and S. Kochemazov. "Finding effective SAT partitionings via black-box optimization". Chapter in book *Black Box Optimization, Machine Learning, and No-Free Lunch Theorems*. (2021)

2021c O. Zaikin and S. Kochemazov. "On black-box optimization in divide-and-conquer SAT solving". *Optimization Methods and Software*. (2021)

2020a O. Zaikin, A. Ignatiev, and J. Marques-Silva. "Branch location problems with Maximum Satisfiability". In *Proc. 24th European Conference on Artificial Intelligence (ECAI'2020)*. (2020)

2020b S. Kochemazov, O. Zaikin, A. Semenov, and V. Kondratiev. "Speeding up CDCL inference with duplicate learnt clauses". In *Proc. 24th European Conference on Artificial Intelligence (ECAI'2020)*. (2020)

2020c A. Semenov, I. Otpuschennikov, I. Gribanova, O. Zaikin, and S. Kochemazov. "Translation of algorithmic descriptions of discrete functions to SAT with applications to cryptanalysis problems". *Logical Methods in Computer Science*. (2020)

2020d S. Kochemazov, O. Zaikin, E. Vatutin, and A. Belyshev. "Enumerating diagonal Latin squares of order up to 9". *Journal of Integer Sequences*. (2020)

2019a O. Zaikin, I. Derevitskii, K. Bochenina, and J. Holyst. "Optimizing spatial accessibility of company branches network with constraints". In *Proc. 19th International Conference on Computational Science (ICCS'19)*. (2019)

2018a A. Semenov, O. Zaikin, I. Otpuschennikov, S. Kochemazov, and A. Ignatiev. "On cryptographic attacks using backdoors for SAT". In *Proc. 32nd AAAI Conference on Artificial Intelligence (AAAI'2018)*. (2018)

2018b S. Kochemazov and O. Zaikin. "ALIAS: a modular tool for finding backdoors for SAT". In *Proc. 21st International Conference on Theory and Applications of Satisfiability Testing (SAT'2018)*. (2018)

2017a O. Zaikin and S. Kochemazov. "An improved SAT-based guess-and-determine attack on the alternating step generator". In *Proc. 20th Information Security Conference (ISC'2017)*. (2017)

2016a I. Otpuschennikov, A. Semenov, I. Gribanova, O. Zaikin, and S. Kochemazov. "Encoding cryptographic functions to SAT using Transalg System". In *Proc. 22nd European Conference on Artificial Intelligence (ECAI'2016)*. (2016)

2016b A. Semenov and O. Zaikin. "Algorithm for finding partitionings of hard variants of Boolean satisfiability problem with application to inversion of some cryptographic functions". *SpringerPlus*. (2016)

2016c O. Zaikin, A. Zhuravlev, S. Kochemazov, and E. Vatutin. "On the construction of triples of diagonal Latin squares of order 10". *Electronic Notes in Discrete Mathematics*. (2016)

Grants

2020–2022 Grant `EP/S015523/1` of the Engineering and Physical Sciences Research Council (EPSRC), United Kingdom

2019–2020 Grant `19-07-00746-a` of Russian Foundation for Basic Research

2016-2020 Grant `16-11-10046` of Russian Science Foundation

2016–2018 Grant `16-07-00155-a` of Russian Foundation for Basic Research

2014–2016 Grant `14-07-00403-a` of Russian Foundation for Basic Research

2011–2012 Grant `11-07-00377-a` of Russian Foundation for Basic Research

2007–2009 Grant 07-01-00400-a of Russian Foundation for Basic Research

Other activity

• PC member of the AAAI Conference on Artificial Intelligence (AAAI) 2024, 2025
• PC member of the International Joint Conference on Artificial Intelligence (IJCAI) 2020, 2021, 2022, 2023, 2024
• PC member of the International Conference on Optimization and Applications (OPTIMA) 2018, 2019, 2020
• PC member of the International Olympiad in Cryptography (NSUCRYPTO) 2023, 2024.
• Reviewer for the following journals: IEEE Transactions on Computers, IEEE Transactions on Cybernetics, European Journal of Operational Research; Discrete Mathematics; Journal of Experimental Algorithmics; Frontiers of Computer Science; Soft Computing; Microprocessors and Microsystems; .
• External reviewer for SAT 2020, 2021; CP 2023; Pragmatics of SAT (POS) 2019, 2021

Languages

Russian	Fluent (native language)
English	Advanced (C1 IELTS)

Computer skills

Programming	C++, C, Python
Parallel computing	Openmp, MPI, BOINC