Zhakshylyk Nurlanov

Doctoral Researcher

Boston, MA (from August 2025)

zh.nurlanov@gmail.com | Zhakshylyk Nurlanov | nurlanov.me | nurlanov-zh | nurlanov-zh | @NurlanovZh

As a doctoral researcher specializing in deep learning robustness, optimization, and computer vision, I have developed reliable AI systems and contributed to cutting-edge projects at Bosch, TUM, and Samsung, with research published in top-tier venues. My expertise lies in designing robust training algorithms, improving AI safety, and advancing computer vision techniques. I am eager to leverage these skills to develop interpretable and trustworthy AI solutions that drive scientific discovery and address complex interdisciplinary challenges.

Education

University of Bonn — *Bonn, Germany*
Ph.D. in Computer Science — *2022 - 2025 (Expected)*
- Research focused on *deep learning robustness and AI safety*
- Advisors: Prof. Florian Bernard and Dr. Frank R. Schmidt (Bosch Center for AI)

Technical University of Munich (TUM) — *Munich, Germany*
M.Sc. in Computer Science — *2019 - 2021*
- GPA: 1.4/1.0 (Top 10%); Courses: Computer Vision, Optimization, Machine Learning & Deep Learning
- Thesis: *Deep Learning for Multi-Graph Matching* (Grade: 1.0), supervised by Prof. Florian Bernard

Moscow Institute of Physics and Technology (MIPT) — *Moscow, Russia*
B.Sc. in Applied Mathematics and Physics — *2015 - 2019*
- GPA: 4.8/5.0 (Honours, Top 5%); Courses: Advanced Mathematics, Computer Science, Physics
- Thesis: *Speech-Driven 3D Facial Avatar Animation*, supervised by Prof. Victor Lempitsky

Experience

Bosch Center for Artificial Intelligence — *Renningen, Germany*
Doctoral Researcher — *12/2021 - Present*
- Developed deep learning models that achieve up to *2× certified robustness* while maintaining high accuracy on image classification benchmarks
- Identified *security vulnerabilities* in large language models (LLMs) through automated red-teaming, achieving near 100% attack success on open-source models and substantially improving cross-model attack transferability

Computer Vision Group, TUM — *Munich, Germany*
Student Research Assistant — *10/2020 - 04/2021*
- Optimized numerical stability of *SO3 transformation algorithms*, contributing to the widely used Sophus library
- Created a *visual odometry system for event cameras*, improving motion estimation in low-light conditions
- Enhanced test coverage for the *visual-based navigation* master course by refining C++ testing frameworks

Samsung R&D Institute — *Moscow, Russia*
Computer Vision Engineer — *06/2018 - 08/2019*
- Designed and trained deep learning models for real-time *speech-driven 3D facial avatar animation*
- Implemented *GAN-based image manipulation* techniques for high-fidelity photorealistic editing
- Built *deep learning pipelines for video action recognition*, reaching production-level accuracy

Publications

1 Jailbreaking LLMs Without Gradients or Priors: Effective Transferable Attacks via Random Local Search — *2025*
Zhakshylyk Nurlanov**, Frank R. Schmidt, Florian Bernard* — ***Preprint

2 Adaptive Certified Training: Towards Better Accuracy-Robustness Tradeoffs — *2024*
Zhakshylyk Nurlanov**, Frank R. Schmidt, Florian Bernard* — ***ECML/PKDD

3 Universe Points Representation Learning for Partial Multi-Graph Matching — *2023*
Zhakshylyk Nurlanov**, Frank R. Schmidt, Florian Bernard* — ***AAAI (Oral)

4 Efficient and Flexible Sublabel-Accurate Energy Minimization *2022*
Zhakshylyk Nurlanov**, Daniel Cremers, Florian Bernard* ***ICPR

5 Exploring SO(3) Logarithmic Map: Degeneracies and Derivatives *2021*
Zhakshylyk Nurlanov ***Tech. Report***

6 Fully Event-Inspired Visual Odometry *2020*
Zhakshylyk Nurlanov**, Nikita Korobov* ***Tech. Report

Patents

- Device and Computer Implemented Method for Machine Learning *2023*
  Frank R. Schmidt, Florian Bernard, ***Zhakshylyk Nurlanov*** ***EP***
- Robust Tracking of Keypoints of Objects in Images *2022*
  Florian Bernard, Frank R. Schmidt, ***Zhakshylyk Nurlanov*** ***DE***
- Method for Generating Head Model Animation From Voice Signal, and Electronic Device for Implementing It *2019*
  I. Glazistov, I. Krotov, ***Z. Nurlanov**, I. Karacharov, A. Simutin, A. Danilevich* ***WO, KR, RU***

Skills

Programming & Development	Python, C++, Matlab, Git, PyTorch, TensorFlow, LSF & SLURM
Research & Communication	Technical Writing, Public Speaking, LaTeX, Power Point
Languages	Kyrgyz (Native), English (Fluent), Russian (Fluent), German (Intermediate)

Honors & Awards

2022 **Travel Stipend** ($ 1000 USD), Committee of ICPR *Montreal, Canada*
2019 **DAAD Master's Scholarship** (Top 5% of Applicants) - € 25000 funding, DAAD *Munich, Germany*
2017 **Scholarship for Excellent Academic Performance** (Top 5%, $ 1200 USD), MIPT *Moscow, Russia*
2015 **Outstanding High School Graduate** (Top 2 of 53,000), National Testing *Kyrgyzstan*
2015 **3rd Place at National Mathematical Olympiad & Participant at IMO** *Kyrgyzstan & Thailand*

Miscellaneous

Reviewer: CVPR 2025, ICLR 2025, ECCV 2024, ICML 2023, ICCV 2023, GCPR 2023, IEEE TNNLS, IEEE TPAMI

Committee Member: Kyrgyz National Mathematical Olympiad (2021 - Present)

Hobbies: chess (national master), basketball, traveling