Zhakshylyk Nurlanov

Ph.D. candidate in machine learning at the University of Bonn. Based in Berlin, Germany.

zh.nurlanov@gmail.com +49 177 85 05 992 nurlanov.me nurlanov-zh nurlanov-zh Google Scholar

Machine learning researcher with a background in applied mathematics and first-author publications at NeurIPS, AAAI, ECML PKDD and ICPR. Research spans image watermarking and provenance, LLM red-teaming, certified robustness, graph matching and numerical optimization, with four patent filings from work at Bosch AI and Samsung R&D. Represented Kyrgyzstan at the 2015 International Mathematical Olympiad; National Master in chess.

EXPERIENCE

Feb 2022 – now
Bonn

University of Bonn, Ph.D. candidate in informatics
Advisor: Florian Bernard

- **VectorMark**: collusion-resistant image fingerprinting with near-orthogonal keys: finds the exact group of ten colluders among a million registered users in 98% of trials, at a 1% false-accusation budget. NeurIPS 2026 Code
- **Image Signatures**: signed provenance inside the pixels: the creator's signature, bound to a fingerprint of the image, shows who created it, when, and whether it was edited. High-capacity robust watermarking with dense rectification. Under review

Dec 2021 – May 2025
Renningen

Bosch Center for Artificial Intelligence, Industrial Ph.D. researcher
Co-advisor: Frank R. Schmidt

- **RAILS**: gradient-free, token-level search for automated LLM red-teaming: 90.2% attack success on Llama 2 (GCG: 43.9%) and transfer to GPT-3.5 and Gemini. ICPR 2026 Patent EP4687056
- **Adaptive certified training**: per-sample certified radii: up to twice the average certified radius at the same clean accuracy on CIFAR-10 and Tiny ImageNet. ECML PKDD 2024 Patent EP4478259 Code
- **Universe points**: cycle-consistent partial multi-graph matching; state of the art in semantic keypoint matching on Pascal VOC, CUB and Willow. AAAI 2023 oral Patent DE102022207076

Oct 2020 – Apr 2021
Munich

TU Munich, Computer Vision Group, Research assistant

- **SO(3) logarithmic map**: numerically stable formulas near π and Jacobians validated by finite differences and automatic differentiation; fixes proposed to Sophus. Technical report Code

Jun 2018 – Aug 2019
Moscow

Samsung R&D Institute, Computer vision engineer

- **Speech-driven 3D avatar animation**: models, real-time demo and training data. Patent WO2021112365
- **Video-based gesture recognition**: models, real-time demo, datasets and annotation tools.

EDUCATION

2022 – now

University of Bonn, Ph.D. candidate in informatics (expected 2027)
Deep learning security and safety. Advisor: Florian Bernard.

2019 – 2021

Technical University of Munich, M.Sc. informatics, with distinction (top 10%)
Thesis: deep partial multi-graph matching. Projects: event-based visual odometry, RGB-D face reconstruction.

2015 – 2019

Moscow Institute of Physics and Technology, B.Sc. applied mathematics and physics, with honours (top 5%)
Thesis: speech-driven 3D facial avatar animation.

PUBLICATIONS

NeurIPS 2026

Beyond Bit Matching: Orthogonal Watermarks for Collusion-Resistant Image Fingerprinting
Z. Nurlanov, T. Weißberg, F. Bernard arXiv Code

Under review

Image Signatures: Signed Provenance in Image Pixels with High-Capacity Watermarking and Dense Rectification
Z. Nurlanov, F. Bernard

ICPR 2026

Jailbreaking LLMs Without Gradients or Priors: Effective and Transferable Attacks
Z. Nurlanov, F. R. Schmidt, F. Bernard arXiv

ECML PKDD 2024

Adaptive Certified Training: Towards Better Accuracy–Robustness Tradeoffs
Z. Nurlanov, F. R. Schmidt, F. Bernard arXiv Code
Earlier version at the ICML 2023 AdvML-Frontiers workshop.

AAAI 2023 — Universe Points Representation Learning for Partial Multi-Graph Matching
Z. Nurlanov, F. R. Schmidt, F. Bernard arXiv
Oral presentation.

ICPR 2022 — Efficient and Flexible Sublabel-Accurate Energy Minimization
Z. Nurlanov, D. Cremers, F. Bernard arXiv Code

TUM report 2021 — Exploring $SO(3)$ Logarithmic Map: Degeneracies and Derivatives
Z. Nurlanov Code

TUM report 2020 — Fully Event-Based Visual Odometry
Z. Nurlanov, N. Korobov Code

PATENT FILINGS

2024 Bosch — Device and computer-implemented method for testing a language model, in particular for operating a computer-controlled machine
From RAILS EP4687056 US20260037749 CN121434763

2023 Bosch — Device and computer-implemented method for machine learning
From Adaptive certified training EP4478259

2022 Bosch — Robust tracking of keypoints of objects in images
From Universe points DE102022207076

2019 Samsung — Method for generating head model animation from voice signal, and electronic device for implementing same
WO2021112365 RU2721180 KR102936559

HONOURS AND SERVICE

2026 — Outstanding Reviewer, CVPR 2026 (top 5% of reviewers)

2025 — University of Bonn Ph.D. scholarship

2019 — DAAD scholarship for master studies (top 5% of applicants)

2015 — International Mathematical Olympiad, Kyrgyz national team; 3rd overall, Kyrgyz National Mathematical Olympiad

2015 — Golden Certificate: 2nd of 53,000 in Kyrgyzstan's national university entrance test

2013 — National Master in chess; bronze medal, Kyrgyz national men's championship

Service — Reviewer for NeurIPS, ICML, ICLR, CVPR, ICCV, ECCV, AAAI, BMVC, ACCV, GCPR, IEEE TPAMI and IEEE TNNLS
Organizer and committee member, Kyrgyz National Mathematical Olympiad and national IMO team selection (since 2021)

OPEN SOURCE

Hugging Face Transformers: fixed the `cache_position` initialization for generation without a cache (merged).
SE(3) tutorial by J. L. Blanco-Claraco: coordinate form of Rodrigues' formula and the SO(3) logarithm at an angle of π (merged).
Sophus: proposed fixes for the SO(3) logarithm near π and its analytical Jacobian.
Own code: VectorMark, adaptive certified training, sublabel-accurate energy minimization, SO(3) logarithm, event-based odometry, face reconstruction.

SKILLS

Programming — Python, C++, NumPy, SciPy, CVXPY, Eigen; numerical optimization, probability, statistics.

Machine learning — PyTorch, TensorFlow, Hugging Face, scikit-learn; robust learning, representation learning, model evaluation.

Vision, geometry — OpenCV, Ceres, Sophus, OpenGV; graph matching, 3D vision, visual odometry.

Tools — Linux, Git, SLURM/LSF, automated tests, LaTeX.

Languages — Kyrgyz and Russian (native), English (fluent), German (B2).