

# Dmytro Zakharov

Applied Mathematics Student | Research Engineer in Deep Learning & Applied Cryptography




 zamdimon.github.io  
 zamdimon

 zakharov2025mp11@student.karazin.ua  
 ZamDimon

 +380-97-712-79-77  
 WL-8aoAAAAAJ  
Kyiv, Ukraine

## EDUCATION

### V. N. Karazin Kharkiv National University

 Applied Mathematics, Bachelor's Degree  2021 – 2025  
(expected)  Kharkiv, Ukraine

- Current GPA: **96/100**.
- Received the **Supreme Council of Ukraine** and **Akhiezer Foundation** scholarships for research activity and academic achievements.
- Consistently taking **top-1** in students' ranking.
- Participating in research conferences, competitions (e.g., SCUDEM), and publishing papers.




### Kharkiv Physics & Mathematics Lyceum #27

 2014 – 2021  Kharkiv, Ukraine

- GPA: **11.8/12.0**.
- Received **two President of Ukraine scholarships** for a junior research paper and outstanding final exam results.
- Graduated from one of the best schools nationally (**top-6** according to 2021 rating) with national exam scores (External Independent Testing) in 4 subjects of **794/800** (**198** in **Math**, **199** in **Physics**, **199** in **English**).

## PROFESSIONAL EXPERIENCE




### Research Engineer in Applied Cryptography

 Distributed Lab  December 2023 – Present (10 months)  Kyiv, Ukraine

**Keywords:** *Research, Cryptography, Lecturing, Zero-Knowledge Theory*

- Researching state-of-the-art technologies in Applied Cryptography and Decentralized (Blockchain) Systems, focusing on low-level optimizations of zero-knowledge protocols and the Mathematics behind them.
- Writing and publishing academic research papers.
- Heading internal lectures (**ZKDL Camp**, see <https://zkdl-camp.github.io/>) on Modern Algebra and Zero-Knowledge Cryptography to improve the company's general Mathematics and research writing level.
- Implementing cutting-edge zkEVM and blockchain scalability cryptographic protocols in **Rust** for leading companies in the Blockchain field.

### Golang Backend Engineer

 Distributed Lab  November 2021 – December 2023 (2 years, 1 month)  Kyiv, Ukraine

**Keywords:** *Backend, Golang, Git, Solidity, Amazon S3, PostgreSQL*

- Developed Backend services for **eight** different projects (with being the Team Lead at **two** of them), ranging from document aggregator service to decentralized exchange statistics processing.
- Implemented numerous internal tools to facilitate the development process.

## RESEARCH ACTIVITY

### Unrecognizable Yet Identifiable: Image Distortion with Preserved Embeddings

**Keywords:** *Contrastive Learning, Cancelable Biometrics, Embedding Model, Siamese Architecture*

- **Journal publication:** Dmytro Zakharov, Oleksandr Kuznetsov, and Emanuele Frontoni. "Unrecognizable yet identifiable: Image distortion with preserved embeddings". In: *Engineering Applications of Artificial Intelligence* (2024). DOI: [10.1016/j.engappai.2024.109164](https://doi.org/10.1016/j.engappai.2024.109164). See [GitHub implementation](#). Preprint URL: <https://arxiv.org/abs/2401.15048>.
- **Conference paper:** Dmytro Zakharov, Oleksandr Kuznetsov, Emanuele Frontoni, and Natalia Kryvinska. "Embedding Non-Distortive Cancelable Face Template Generation". 2024. arXiv: [2402.02540](https://arxiv.org/abs/2402.02540) [[cs.CV](#)]. *The full paper is **accepted** and awarded as the **Best Paper** at **The 23rd International Conference on Artificial Intelligence and Soft Computing**.*

### Deep Learning-based Biometric Cryptographic Key Generation

**Keywords:** *Triplet Loss, Biometrics, Cybersecurity, Fuzzy Extractor, Code-based Cryptosystems*

- **Journal publication:** Oleksandr Kuznetsov, Dmytro Zakharov, and Emanuele Frontoni. "Deep learning-based biometric cryptographic key generation with post-quantum security". In: *Multimedia Tools and Applications* (2023). doi: [10.1007/s11042-023-17714-7](https://doi.org/10.1007/s11042-023-17714-7). URL: <https://doi.org/10.1007/s11042-023-17714-7>.
- **Conference publication:** Alexandr Kuznetsov, Dmytro Zakharov, Emanuele Frontoni, Luca Romeo, and Riccardo Rosati. "Deep Learning Based Fuzzy Extractor for Generating Strong Keys from Biometric Face Images". In: *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. 2022, pp. 421426. doi: [10.1109/PICST57299.2022.10238643](https://doi.org/10.1109/PICST57299.2022.10238643).
- **Preprint:** URL: [doi.org/10.21203/rs.3.rs-2913502/v1](https://doi.org/10.21203/rs.3.rs-2913502/v1).

## AttackNet: Convolutional Neural Network for Liveness Detection

**Keywords:** *Deep Learning, Convolutional Neural Network, Liveness Detection, Cybersecurity*

- **Journal publication:** Oleksandr Kuznetsov, Dmytro Zakharov, Emanuele Frontoni, Andrea Maranesi. "AttackNet: Enhancing biometric security via tailored convolutional neural network architectures for liveness detection". In: *Elsevier Computers & Security* (2024). Vol. 141. 103828. DOI: [10.1016/j.cose.2024.103828](https://doi.org/10.1016/j.cose.2024.103828).
- **Conference publication:** Oleksandr Kuznetsov, Dmytro Zakharov, Emanuele Frontoni, Andrea Maranesi, and Serhii Bohucharskyi. "Cross-Database Liveness Detection: Insights from Comparative Biometric Analysis". In: *SCIA 2023, Lviv, Ukraine, November 9, 2023*. Vol. 3608. CEUR Workshop Proceedings. CEUR-WS.org, 2023, pp. 250263. URL: <https://ceur-ws.org/Vol-3608/paper19.pdf>.

## Cryptographic Protocols on top of Bitcoin

**Keywords:** *Bitcoin, Zero-Knowledge Proofs, Low-Level Optimizations, L2 Layer*

- Dmytro Zakharov, Oleksandr Kurbatov, Manish Bista, Belove Bist. "Optimizing Big Integer Multiplication on Bitcoin: Introducing  $w$ -windowed Approach". In: *Cryptology ePrint Archive*, URL: <https://eprint.iacr.org/2024/1236>.
- Oleksandr Kurbatov, Dmytro Zakharov, Anton Levochko, Kyrylo Riabov, Bohdan Skriabin. "Multichain Taprootized Atomic Swaps: Introducing Untraceability through Zero-Knowledge Proofs". arXiv preprint [arXiv:2402.16735](https://arxiv.org/abs/2402.16735) (2024). *Currently in review to IET Blockchain*.

## VOLUNTEERING

### Ukraine Global Scholars, Finalist 2021

**Keywords:** *Teaching, Lecturing, Test Writing*

- One of 56 finalists out of 550 applicants selected through a rigorous 3-stage selection process focusing on academic skills, extracurricular achievements, and character.
- Led a **Mathematics test creation team** that composed an exam for 300+ test takers to assess their Mathematics knowledge during the application process to a leading non-profit organization focused on helping students obtain scholarships at the best educational institutions around the globe.
- Helped in organizing SAT School — classes that help students obtain a high score on the English part of the SAT exam

## PROJECTS

### ZKDL Camp

Heading Distributed Lab internal in-depth **lectures** on zero-knowledge proofs and cryptography. Reviewing and editing lecture notes, composing tests and practical exercises:

<https://zkdl-camp.github.io/>

### Biometrics Distortion Generator in Python

**Python** source code for the "Unrecognizable Yet Identifiable: Image Distortion with Preserved Embeddings" paper. Contains a well-documented description of all the math and neural network architectures from the paper:

<https://github.com/ZamDimon/distortion-generator>

### $w$ -width Big Integer Multiplication on Bitcoin

**Rust** implementation of an optimized 254-bit integer multiplication on the custom non-Turing-complete stack-based language used in Bitcoin:

<https://github.com/distributed-lab/bitcoin-window-mul>

### Presentations and Talks

My presentations and talks at Distributed Lab on various Deep Learning and Cryptography topics:

<https://github.com/ZamDimon/presentations-and-talks>

## SCHOOL COMPETITIONS

### International Research competition I-FEST – Silver Medal

🇹🇺Tunisia | 📅Nov 2021

International research competition, 40+ countries, 1000+ participants.

### European Union Contest for Young Scientists (EUCYS)

🇪🇸Spain | 📅Sep 2021

Biggest European Union scientific research competition with 40+ countries.

### International Zhautykov Physics Olympiad – Bronze medal

🇰🇿Kazakhstan | 📅Jan 2021

International Olympiad with 20+ participating countries.

## LANGUAGES

### Ukrainian

Native

### English

C2, TOEFL: 113/120, SAT: 1500/1600

### German

B2, took Nürnberger Haus courses