Dmytro Zakharov

Cryptography Engineer | Post-Quantum and Zero-Knowledge Cryptography

zamdimon.github.io | zamdmytro@gmail.com | Google Scholar
zamdimon | ZamDimon | +380-97-712-79-77 | Valencia, Spain

EDUCATION

V. N. Karazin Kharkiv National University

Applied Mathematics, Master's Degree | Sep 2026 – Jun 2028 (expected) | Kharkiv, Ukraine

- Studying Statistics, Optimization and Control Theory, Deep Learning, and Mathematical Modelling.

V. N. Karazin Kharkiv National University

Applied Mathematics, Bachelor's Degree | Sep 2021 – Jun 2025 | Kharkiv, Ukraine

- Cumulative GPA: **96/100** (ranked **Top-1** in cohort).
- **Thesis:** *"Applications of Kolmogorov-Arnold Convolutional Neural Networks to Computer Vision Problems"*.
- Awarded the **Supreme Council of Ukraine** and **Akhiezer Foundation** Scholarships for outstanding research work.

Kyiv School of Economics

Pure Mathematics, Master's Coursework | Sep 2025 – May 2026 | Kyiv, Ukraine

- GPA: **92/100**.
- Advanced coursework: Algebraic Geometry, Homological Algebra, Sheaf Theory, Commutative Algebra, Algebraic Number Theory, Elliptic Curves, Ergodic Theory.

PROFESSIONAL EXPERIENCE

Cryptography Researcher

Blockstream | January 2026 – Present | Remote (Valencia, Spain)

Keywords: *Post-Quantum Cryptography, Lattice-Based Schemes, ZK-SNARKs, Education*

- Conducting research on post-quantum cryptography, specifically evaluating the concrete security and efficiency of **lattice-based signature schemes**.
- Co-authored comprehensive survey on lattice-based signatures for Bitcoin protocol integration.
- Leading academic workshops and seminars on post-quantum zero-knowledge proving systems.

R&D Engineer in Applied Cryptography

Distributed Lab | June 2023 – January 2026 (2 years, 7 months) | Kyiv, Ukraine

Keywords: *Zero-Knowledge ML, Circuit Optimization, Rust*

- Led design and Rust implementation of **Bionetta**, a client-side Zero-Knowledge Machine Learning (ZKML) framework utilizing UltraGroth and custom R1CS arithmetizations.
- Developed low-level optimizations for zero-knowledge proving systems, including PlonK-based circuits for elliptic curve pairing, addition, and scalar multiplication.
- Researched BitVM2-based optimistic verifiable computation on Bitcoin.
- Programmed and delivered the internal **ZKDL Camp** lecture series on Modern Algebra, Field Extensions, and zk-SNARK protocols (Groth16, PlonK, GKR).

Golang Backend Engineer

Distributed Lab | November 2021 – June 2023 (1 year, 7 months) | Kyiv, Ukraine

Keywords: *Golang, PostgreSQL, Docker, Decentralized Systems*

- Designed and led the development of microservices, statistical backend engines, and cryptographic transaction aggregation tools across 8+ client projects.
- Built secure KYC verification workflows, deposit/withdrawal pipelines, and automated analytics indexers for decentralized marketplaces and crowdfunding platforms.
- Built backend infrastructure interfacing with custom Solidity smart contracts and implemented cross-chain bridge logic using the custom smart contract language.

PUBLICATIONS & PREPRINTS

Lattice-based Signature Schemes for Bitcoin

Keywords: *Lattice-based Cryptography, Post-Quantum Security, Signatures, Bitcoin*

- **Dmytro Zakharov**, Mikhail Kudinov, Viktoria Balatska, Yaroslava Chopa. In: *Cryptology ePrint Archive*, Report 2026/1628 (2026). URL: eprint.iacr.org/2026/1628.

Bionetta: Efficient Client-Side Zero-Knowledge Machine Learning Proving

Keywords: *ZKML, UltraGroth, Privacy-Preserving AI, R1CS, Succinct Proofs*

- **Dmytro Zakharov**, Oleksandr Kurbatov, Lasha Antadze, Lev Soukhanov, Artem Sdobnov, Yevhenii Sekhin, Vitalii Volovyk. In: *arXiv preprint arXiv:2510.06784* (2025). URL: arXiv:2510.06784 (**in submission**).

Identifiable Yet Recognizable: Image Distortion with Preserved Embeddings

Keywords: *Biometric Privacy, Cancelable Biometrics, Siamese Networks, Representation Learning*

- **Journal Publication: Dmytro Zakharov**, Oleksandr Kuznetsov, Emanuele Frontoni. In: *Elsevier Engineering Applications of Artificial Intelligence* (2024). DOI: 10.1016/j.engappai.2024.109164.
- **Conference Paper: Dmytro Zakharov** et al. In: *23rd International Conference on Artificial Intelligence and Soft Computing (ICAISC)*, Springer (2024). **Best Paper Award**. DOI: 10.1007/978-3-031-84356-3_18.

Optimizing Big Integer Multiplication on Bitcoin: Introducing w-Windowed Approach

Keywords: *Arithmetic Optimization, Stack Languages, Bitcoin Script, Low-Level Cryptography*

- **Dmytro Zakharov**, Oleksandr Kurbatov, Manish Bist, Belove Bist. In: *Cryptology ePrint Archive*, Report 2024/1236 (2024). URL: eprint.iacr.org/2024/1236.

AttackNet: Enhancing Biometric Security via CNNs for Liveness Detection

Keywords: *Deep Learning, Anti-Spoofing, Cybersecurity, Computer Vision*

- Oleksandr Kuznetsov, **Dmytro Zakharov**, Emanuele Frontoni, Andrea Maranesi. In: *Elsevier Computers & Security*, Vol. 141 (2024). DOI: 10.1016/j.cose.2024.103828.

Deep Learning-Based Biometric Cryptographic Key Generation with Post-Quantum Security

Keywords: *Fuzzy Extractor, Triplet Loss, Post-Quantum Cryptography, Code-Based Cryptosystems*

- Oleksandr Kuznetsov, **Dmytro Zakharov**, Emanuele Frontoni. In: *Springer Multimedia Tools and Applications* (2023). DOI: 10.1007/s11042-023-17714-7.
- **Conference Paper:** IEEE 9th PIC S&T (2022). DOI: 10.1109/PICST57299.2022.10238643.

TEACHING & ACADEMIC OUTREACH

ZKDL Book: Zero-Knowledge Proofs Course

Blockstream / Distributed Lab 2023 – Present

Keywords: *Textbook, Open-Source, zk-SNARKs*

- Co-authoring open-source lecture notes and textbook covering theoretical foundations of ZK protocols (Groth16, PlonK, GKR), polynomial commitments, and underlying abstract algebra.
- **Repository:** BlockstreamResearch/zk-book.

Cryptography: A Modern Approach

Distributed Lab / University Lectures 2023 – 2024

Keywords: *Curriculum Design, Lecturing*

- Co-designed curriculum and delivered lectures for Ukrainian university students on Symmetric/Asymmetric Cryptography, Finite Field Theory, Digital Signatures, and Zero-Knowledge Proofs.
- **Repository:** distributed-lab/crypto-lectures.

TECHNICAL & MATHEMATICAL SKILLS

Cryptography
Lattice-Based Cryptography, Zero-Knowledge Proofs (pairing and lattice-based), Bitcoin, Low-level Optimization.

Machine Learning & Privacy
Privacy-Preserving ML, Computer Vision, Triplet Loss, Biometrics, Neural Network Security.

Programming Languages
Rust (Advanced), Python (PyTorch, NumPy, SciPy), Golang, C++, LaTeX, Wolfram Language.

Developer Tools
Git, Linux, Docker, PostgreSQL, Amazon AWS, CI/CD Pipelines.

LANGUAGES & STANDARDIZED TESTS

Ukrainian
Native

English
CEFR C1–C2
*TOEFL: **113/120***
*SAT: **1500/1600** (Math: **800/800**)*

German
CEFR B2
Completed Das Nürnberger Haus (Goethe-Institut Partner) courses