Efe İzbudak

Website: ephemer4l.me
Email: efe@liberior.org
GitHub: github.com/ephemer4l

INTERESTS

Higher structures, lattice-based cryptography, homomorphic encryption

EDUCATION

Middle East Technical University — Ankara, TR
BSc in Mathematics, GPA: 4.00/4.00 — 2022–2026

RESEARCH EXPERIENCE

Sabanci University — İstanbul, TR
Cryptography and Information Security Group — August 29, 2024 – Current

- Investigating algebraic and approximation-theoretic techniques to optimize homomorphic encryption scheme implementations.

Sabanci University — İstanbul, TR
Program for Undergraduate Research (PURE) — Summer 2024, 2025

- Developing accelerators for homomorphic encryption, 2024 Report, 2025 Report
- Supervisor: Erkay Savaş
- 2024: Implemented CKKS bootstrapping and developed GPU-accelerated algorithms (FFT, Karatsuba).
- 2025: Supervised undergraduate students on implementing the FHE schemes (TFHE, scheme switching, matrix multiplication)

PUBLICATIONS

[1] **E. İzbudak** and A. Ş. Özcan, "Practical bootstrapping of CKKS ciphertexts with HEonGPU", Work in progress, 2025.

LEARNING SEMINARS

Derived Algebraic Geometry — Online
Alexander Zahrer, Lucy Grossman, Marcus Nicolas, Outline — Spring 2025 – Current

Higher Structures — Middle East Technical University
Kadri İlker Berktav, 2 talks contributed. — Spring 2025 – Current

Recent papers on RLWE/PLWE problems — Online
Ferruh Özbudak, Kamer Kaya, Selim Kırbıyık, 3 talks contributed. — Fall 2024

Serre's Local Algebra — Middle East Technical University
Özgür Kişisel, 2 talks contributed, notes (for my talks). — Spring 2024

Categorical Quantum Mechanics — Bilkent University
Cihan Okay — Spring 2024

CERTIFICATES

- LFD103, The Linux Foundation, February 2023
- LFC108, The Linux Foundation, March 2025

SCHOLARSHIPS

- TMD Cahit Arf Scholar — January 2024 - Current
- TOG-Bezmen Merit Scholar — 2022 - Current

SELECTED TALKS

All Morphisms Are Equal, But Some Morphisms Are More Equal Than Others — Sabanci University
DRP Türkiye, Report, Slides — September 5, 2024

Sparse Packing for CKKS — Sabanci University
Slides — Summer 2024

Fast Multiplication and PLWE-RLWE Equivalence — Online
Slides — Fall 2024

Lattice-Based Foundations of Homomorphic Encryption — Middle East Technical University
Slides — Fall 2024

Cryptanalysis of PLWE Based on Zero-Trace Quadratic Roots — Online
Slides — Winter 2025

CONFERENCES & WORKSHOPS

- *Higher Structures Workshop* — September 8-12, 2025, Hamburg, DE
- *Higher Structures Summer School* — September 1-5, 2025, Hamburg, DE
- *Random Real Algebraic Geometry Summer School* — August 11-15, 2025, İzmir, TR
- *Thirtieth Gökova Geometry / Topology Conference* — May 25-30, 2025, Muğla, TR
- *Mapping Class Groups and Beyond* — May 14-18, 2025, Ankara, TR
- *Real World Crypto Symposium* — March 26-28, 2025, Sofia, BG
- *4th Annual FHE.org Conference* — March 25, 2025, Sofia, BG
- *8th Homomorphic Encryption Standards Meeting* — March 23, 2025, İstanbul, TR

COMMUNITY CONTRIBUTIONS

- Tor Project, Relay Operator — December 2020 – Current
  Supporting global internet freedom by maintaining a secure bridge.

- Gentoo, Proxied Maintainer — August 2022 – Current
  Maintained packages: `sc-im`, `mutt-wizard`, `libxlsxwriter`

- Qubes, Techical Documentation Writer — November 2020 – December 2020
  Authored the technical documentation for the split-ssh feature.

WORK EXPERIENCE

Founding projects

- Libeiror.org, Founder, System Administrator — February 2023 – January 2024
  Liberior was an organization providing secure and free e-mail/XMPP accounts.

- Liberpub, Founder, System Administrator — July 2022 – January 2024
  Liberpub was an online printing service with no initial cost for the author.

Freelance experience

- Upwork, Freelance Software Developer — July 2022 – September 2023
  Projects include: LaTeX to MathJax conversion, PDF harvesting and manipulation

SKILLS

- Python, Rust, Shell Scripting
- LaTeX, Git, Linux Administration (Gentoo)
- Cryptography, Digital Forensics

LANGUAGES

- **English:** Fluent
- **French:** Basic reading
- **Turkish:** Native