Efe İzbudak

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

INTERESTS

Higher structures, homotopy theory, 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 bootstrapping in the CKKS homomorphic encryption scheme.

Sabanci University — İstanbul, TR
Program for Undergraduate Research (PURE) — Summer 2024
- Developing accelerators for homomorphic encryption
- Supervisor: Erkay Savaş

PUBLICATIONS & PREPRINTS

[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 (incomplete). — 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 AND AWARDS

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

Selected Expository Presentations & 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 Attended

- *Random Real Algebraic Geometry* 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 & Open Source 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