

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
BSc in Mathematics, GPA: 4.00/4.00

Ankara, TR
2022–2026

RESEARCH EXPERIENCE

Sabanci University
Cryptography and Information Security Group

İstanbul, TR
August 29, 2024 – Current

- Investigating acceleration techniques for CKKS bootstrapping

Sabanci University
Program for Undergraduate Research (PURE)

İstanbul, TR
Summer 2024

- Developing accelerators for homomorphic encryption
- Supervisor: Erkey Savaş

PUBLICATIONS

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

LEARNING SEMINARS

Derived Algebraic Geometry
Alexander Zahrer, Lucy Grossman, Marcus Nicolas, Outline

Online
Spring 2025 – Current

Higher Structures
Kadri İlker Berktav, 2 talks contributed.

Middle East Technical University
Spring 2025 – Current

Recent papers on RLWE/PLWE problems
Ferruh Özbudak, Kamer Kaya, Selim Kırbyık, 3 talks contributed.

Online
September 28, 2024 – November 13, 2024

Serre’s Local Algebra
Özgür Kişisel, 2 talks contributed, notes (incomplete).

Middle East Technical University
Spring 2024

Categorical Quantum Mechanics
Cihan Okay

Bilkent University
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

<i>All Morphisms Are Equal, But Some Morphisms Are More Equal Than Others</i> DRP Türkiye, Report, Slides	Sabanci University September 5, 2024
<i>Sparse Packing for CKKS</i> Slides	Sabanci University Summer 2024
<i>Fast Multiplication and PLWE-RLWE Equivalence</i> Slides	Online Fall 2024
<i>Lattice-Based Foundations of Homomorphic Encryption</i> Slides	Middle East Technical University Fall 2024
<i>Cryptanalysis of PLWE Based on Zero-Trace Quadratic Roots</i> Slides	Online Winter 2025

CONFERENCES & WORKSHOPS ATTENDED

• <i>Thirtieth Gökova Geometry / Topology Conference</i>	May 25-30, 2025, Muğla, TR
• <i>Mapping Class Groups and Beyond</i>	May 14-18, 2025, Ankara, TR
• <i>Real World Crypto Symposium</i>	March 26-28, 2025, Sofia, BG
• <i>4th Annual FHE.org Conference</i>	March 25, 2025, Sofia, BG
• <i>8th Homomorphic Encryption Standards Meeting</i>	March 23, 2025, İstanbul, TR

MISCELLANEOUS

Community contributions

• Tor Project, Relay Operator <i>Supporting global internet freedom by maintaining a secure bridge.</i>	December 2020 – Current
• Gentoo, Proxied Maintainer <i>Maintained packages: <code>sc-im</code>, <code>mutt-wizard</code>, <code>libxlszwriter</code></i>	August 2022 – Current
• Qubes, Technical Documentation Writer <i>We have produced the <code>split-ssh</code> method.</i>	November 2020 – December 2020

Founding projects

• Libeior.org, Founder, System Administrator <i>Libeior was an organization providing secure and free e-mail/XMPP accounts.</i>	February 2023 – January 2024
• Liberpub, Founder, System Administrator <i>Liberpub was an online printing service with no initial cost for the author.</i>	July 2022 – January 2024

Freelance experience

• Upwork, Freelance Software Developer <i>Projects include: \LaTeX to MathJax conversion, PDF harvesting and manipulation</i>	July 2022 – September 2023
--	----------------------------

SKILLS

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

LANGUAGES

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