Lattice Cryptography

Mustafa Kırcalı

April 13, 2026

Abstract

The rapid progress in quantum computing has created a serious challenge for many classical public-key cryptosystems. This has led to the development of post-quantum cryptography, a research area devoted to constructing cryptographic systems that remain secure even against quantum computers. Among the most prominent candidates in this area, lattice-based cryptography stands out because of its strong theoretical foundations and practical efficiency.

In this seminar, we present a general introduction to lattice-based cryptography from a motivational perspective. We explain why lattices have become central objects in post-quantum cryptography, discuss the hard mathematical problems on which their security is based, and outline how these problems give rise to useful cryptographic constructions.

MSC Number: 11T71, 94A60, 68P25

Keywords: Post-quantum cryptography, lattice-based cryptography, computational hardness, public-key cryptography

Address: *Department of Mathematics, Izmir University of Economics, İzmir, Türkiye. E-mail: mustafa.kircali@ieu.edu.tr*

References

[1] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, Journal of the ACM, 56(6), 2009.

[2] D. Micciancio and O. Regev, *Lattice-based Cryptography*, in *Post-Quantum Cryptography*, Springer, 2009, pp. 147–191.

[3] C. Peikert, *A Decade of Lattice Cryptography*, Foundations and Trends in Theoretical Computer Science, 10(4), 2016, pp. 283–424.