Speaker: Eda Kırımlı
Title: Isogeny graphs of abelian surfaces

Abstract. Isogeny-based cryptography is an active research area in post-quantum cryptography, and its security depends on variants of isogeny problems, namely the problem of finding an explicit isogeny between two abelian varieties. Although much of the research focused on isogenies of elliptic curves so far, it is mathematically interesting to understand isogeny graphs in dimension 2 in full generality, and the recent attacks using isogenies in higher dimensions switched the attention to dimension 2 more than ever.

Unlike known methods, we use very geometrical and arithmetical objects called Refined Humbert Invariants defined by Kani. We will propose possible promising applications using Refined Humbert Invariants of abelian surfaces. We will investigate how to understand isogeny graphs of abelian varieties, and explain possible applications such as determining minimum walks, finding split abelian surfaces, a security reduction to computing the degree of an isogeny, and multilinear maps.

N.B. This is joint work in progress with Harun Kır.