

**Speaker:** Yan Bo Ti

**Title:** Isogeny-based cryptography on the (abelian) surface

**Abstract.** It is an understatement to say that isogeny-based cryptography has been on a journey of ups and downs. Through the course of this journey, various techniques have been used to analyse isogeny-based cryptosystems. One of which, is using genus two methods to examine and build isogeny-based cryptosystems, and ultimately break one of the most promising key exchange schemes, SIDH. In this talk, we will look at cameos and appearances of genus two in isogeny-based cryptography. We will survey the landscape and see how genus two can be used constructively and sometimes destructively on isogeny-based cryptography.