

Department of Mathematics, BGU

AGNT

On Wednesday, May ,29 2024

At 14:10 – 15:00

In 101-

Eyal Goren (McGill University)

will talk about

Supersingular elliptic curves, quaternion algebras and some applications to cryptography

Abstract: Part of the talk is expository: I will explain how supersingular isogeny graphs can be used to construct cryptographic hash functions and survey some of the rich mathematics involved. Then, with this motivation in mind, I will discuss two recent theorems by Jonathan Love and myself. The first concerns the generation of maximal orders by elements of particular norms. The second states that maximal orders of elliptic curves are determined by their theta functions.