The nodes of an isogeny graph are elliptic curves, and the edges are special maps between elliptic curves called isogenies. Knowing which hash values are most likely informs us of potential security weaknesses in the hash function. We will use stochastic matrices to compute the expected

$$\pi = \lim_{n \to \infty} \pi_0 A^n$$

completely describes all possible probability distributions of the CGL hash function. We will use this theorem to evaluate the collision resistance of the CGL hash function and compare this to the collision resistance of an "ideal" hash function.

Wednesday, December 7th at 7 PM

Join at Park 245 or via Zoom

Snacks in the Math Lounge at 6:30 PM, before the talk begins!

Zoom Link: https://brynmawr-edu.zoom.us/j/9580798217?pwd=aXB3MnFZMUUyWDQ1S1d3TGozc0t5Zz09