BRYN MAWR DISTRESSING MATH COLLECTIVE

PROBABILITY DISTRIBUTIONS FOR THE ELLIPTIC CURVES CGL HASH FUNCTION

KARA FAGERSTROM '22

Hash functions map data of arbitrary length to data of predetermined length. Good hash functions are hard to predict, making them useful in cryptography. We are interested in the elliptic curve Charles-Goren-Lauter (CGL) hash function, which maps a bitstring to an elliptic curve by traversing an input determined path through an isogeny graph. 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 probability distributions of the hash values. Then we will generalize our experimental data into a theorem that 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 8th 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/95807982212?pwd=aXBBMnFZMUUyWDQ1S1d3TGozc0t5Zz09