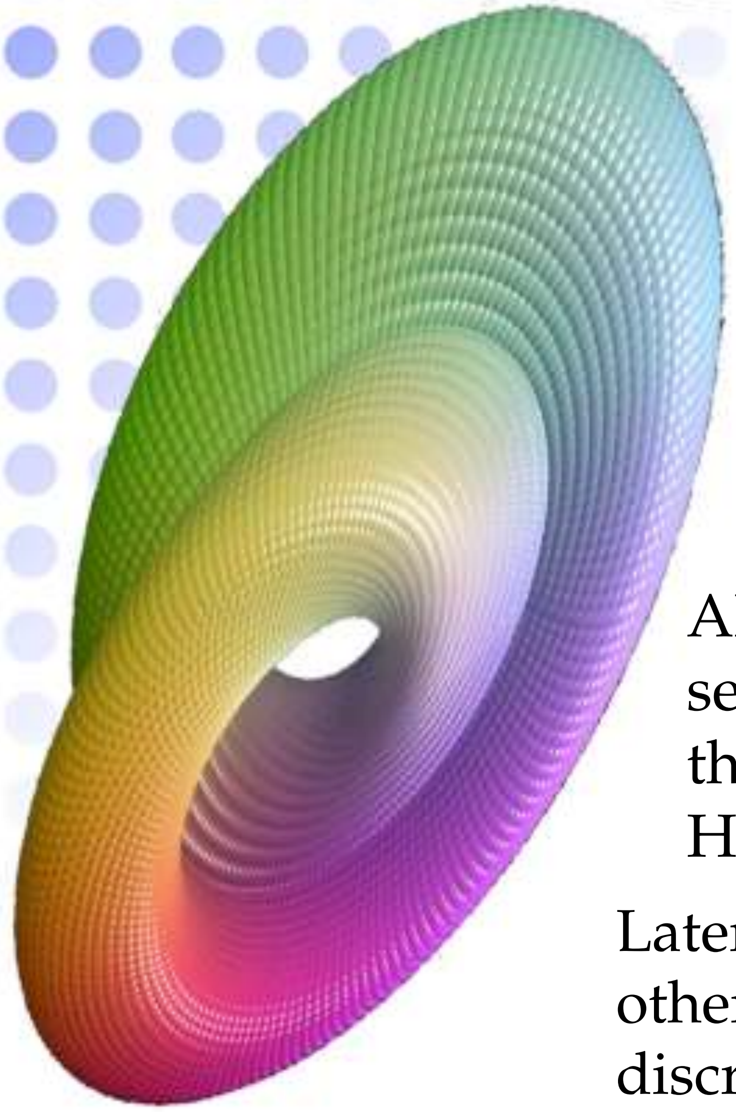
Michigan Math Club

Thursday at 4pm in EH1360

Free raffle prizes afterwards!



How to Share and Compute on Secret Data

Quang Dao • 27 January 2022

Alice has a secret that she wishes to safeguard. She wants to divide the secret into n shares and send them to her trusted contacts so that any t of them can recover the secret, but no $(t-1)$ of them learn anything about it. How can this be done?

Later on, Alice wishes to compare her salary with others in her company to find out whether wage discrimination has taken place. However, she respects the privacy of her colleagues and only wants to learn the conclusion, not their individual salaries. Can Alice fulfill her request?

We will talk about a solution to those two problems, which comes from an area of cryptography called secure multi-party computation. No prerequisite is required except for an understanding of polynomials and a healthy dose of curiosity!