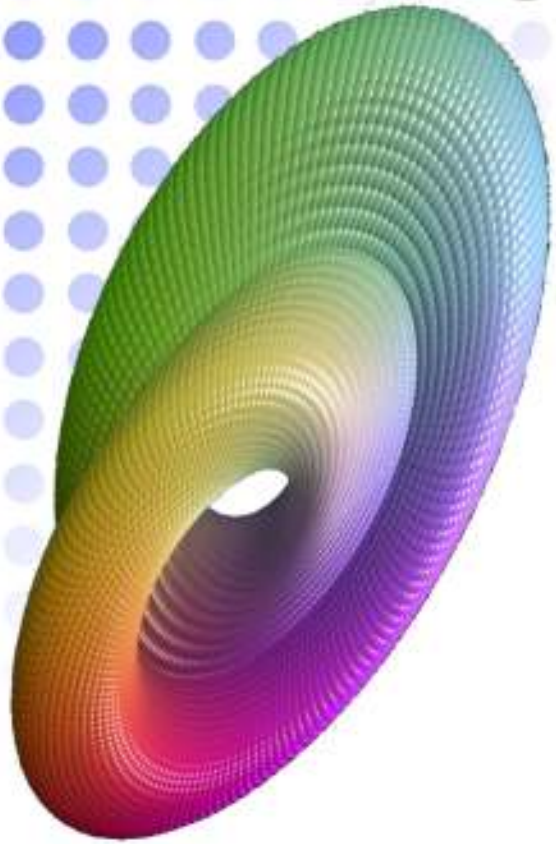
Michigan Math Club

Thursday at 4pm in the Commons

Free Pizza and Pop



Trusted third parties

John Wiltshire-Gordon

Abstract for 12 September

Three millionaires are having a drink when the conversation turns to money. "I wonder which of us is richest," muses the first. "But how can we ever find out? None of us want to reveal such sensitive financial information," observes the second. "Maybe there's a method that will keep our information private..." speculates the third. And even though those particular millionaires have been dead for thirty years, we still study their predicament today.

The first part of this talk is about secure multiparty computation: how to compute when the data are sensitive or the parties are untrustworthy. In the second part, we offer results towards the algorithmic simulation of a trusted third party.

This talk draws on mathematical ideas from probability theory, algebraic geometry, Galois theory, multilinear algebra, and other areas.