The Math/Stats Colloquium
Department of Mathematics and Statistics
San José State University

Yan X. Zhang

SJSU

Folding Computation into Fewer Computations

WED MAR 06, 2024, MH320

Abstract: In the context of interactive proofs and "zero knowledge", a *folding scheme* (popularized by Nova) is a way to combine multiple instances of a constraint system into a single instance. In English, this means you can check that multiple computations were done correctly by checking a single computation, a claim that should feel very suspicious. I will present the main ideas of folding and (as joint work with Aard Vark) how it can be applied to custom computation and "lookups", a useful concept in modern zero knowledge engineering.

Background: Familiarity with polynomials (as in high school algebra). No background in interactive proofs or cryptography required.

About the speaker: Yan X. Zhang is an associate professor at San José State University and the director of the CAMCOS program. He has worked on and organized blockchain research with outside entities including the Ethereum Foundation, Stanford CBR (Center for Blockchain Research), and 0xPARC.

SNACKS IN MACQUARRIE HALL 331B AT 2:40PM
TALK STARTS AT 3:00PM

For more information, see our full schedule at:

`http://www.timhsu.net/colloq/`