Yan X. Zhang

SJSU

Automated Cryptography

OCTOBER 24, 2018, MH320

Abstract: In many applications of cryptography, people want to exchange secrets and to have security guarantees, such as when someone is able to know a secret and when someone does not. We define a framework that embeds such a situation into a "blueprint" and show that all these blueprints can be satisfied. As a possibly surprising consequence, we show that we can generate explicit algorithms automatically from just the "blueprints", somewhat like proving mathematical theorems automatically.

Background: Discrete math (Math 42). No experience with cryptography required.

About the speaker: Yan X. Zhang is an assistant professor of mathematics at SJSU. His main research interest is discrete mathematics, especially in applications of pure math into applied fields. His recent research interests has been on cryptography and the blockchain.

SNACKS IN MH331B AT 2:30 PM
TALK STARTS AT 3:00 PM

For more information, see our full schedule at:

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